Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 19

Name Processing of personal data within the framework of the Data Protection Office tasks, duties and activities

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 07 - Data Protection Office

Entity Name - Processor (Entities)

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft, Microsoft	

OpenText

External processors	
Name OpenText	

OneTrust

External processors

Name	
OneTrust	

Description of the processing

Description The EPO’s Data Protection Office (DPO) processes personal data in order to carry out the tasks and duties assigned to it by the Service Regulations for permanent and other employees of the EPO (Service Regulations), the DPR, other rules, administrative instructions and decisions adopted by the President of the Office and additional operational documents governing the processing of personal data at the EPO.

In the performance of its tasks, the DPO may process any category of personal data (including special categories of personal data) provided by EPO staff members or externals regarding themselves or third parties. It includes information exchanged such as the description of concerns, personal case, circumstances, description of facts, opinions, assessments, etc.

Personal data may be stored in one or more document management tools used by the DPO to perform its tasks, namely on the EPO’s servers and/or in Microsoft Office cloud systems and/or in the Data Protection Tool (DP Tool):

- all data subjects’ enquiries, DPO opinions, advice, recommendations and consultations, and related communications (together with supplementary documentation, as the case may be) received or sent by the DPO are stored in Outlook in folders separated by year and/or on SharePoint 2019 and are only accessible to authorised staff. They are afterwards archived in MatterSphere with a unique identifier assigned to them
- personal data in relation to records of processing activities are stored in the DP Tool
- where necessary, documents (e.g. drafts of operational documents, awareness-raising materials) may also be stored on SharePoint 2019
- when required to do so by internal workflows, personal data may also be entered in OpenText

For more information regarding the processing of personal data by these tools, please refer to the dedicated record(s).

The DPO manages the Data Protection Liaisons (DPLs) network, DPLs are appointed by each delegated controller to be their contact point in relation to data protection matters.

The DPO may also be requested by the Data Protection Board (DPB) to provide support, to that extent the DPO may process, on a strictly need-to-know basis, personal data such as the details of the data subject filing a complaint, personal data contained in allegations, and other categories of personal data depending on the case. For more information on the processing of personal data by the DPB, please refer to the relevant record.

The processing is not intended to be used for any automated individual decision-making.

Data Retention Personal data will be kept only for the time needed to achieve the purpose(s) for which they are processed.

Purpose of Processing carrying out data protection investigations and audits, raising awareness/ providing training on data protection matters, providing opinions, advice, recommendations and responses regarding consultations received from the relevant controller, delegated controllers, processors or any body set up under Article 2 of the Service Regulations, offering support to the DPB in carrying out its function under the DPR, assisting organisational units with (internal or external) data subjects’ enquiries (meaning queries, requests to exercise data subject’ rights, requests for review by the delegated controller, complaints of alleged infringement of the DPR, including potential reports on personal data breaches), co-operating with other organs of the European Patent Organisation (i.e. the Administrative Council), European Union institutions, bodies, offices and agencies and/or other international organisations, - maintaining the Data Protection Register within the DP Tool and SharePoint 2019 (https://sharepoint2019.internal.epo.org/sites/DPOREG/Lists/DPORegisterintranet/AllItems.aspx) o Records involving the processing of external data subjects’ personal data are publicly accessible on the EPO website (https://documents.epo.org/projects/babylon/eponet.nsf/0/B8C31CF8AC6C19D8C12587AD002F98CB/$FILE/data_protection_register_en.pdf). The only personal data processed in this context are the cookies used on the EPO website., assessing risks for individuals resulting from personal data breaches, managing the DPLs network

Personal data related to records inserted in the DP Tool/SharePoint 2019 will be stored for as long as the processing is operational. After that date, the record will be deleted from the public Register but archived for a period of 5 years for reasons of possible formal appeals and litigation procedures.

Personal data related to co-operation with external and internal stakeholders will be stored in the document management tool(s) for a maximum of 5 years after the closure of the case.

Personal data related to DPO opinions, advice, recommendations, consultation and related communications will be stored in the document management tool(s) for a maximum of 5 years after the closure of the consultation or provision of the opinion, advice or recommendation.

Personal data related to data subject enquiries (internal and external) will be stored in the document management tool(s) for a maximum of 10 years after the closure of the enquiry.

Personal data related to data protection investigations will be stored in the document management tool(s) for 10 years after the closure of the investigation.

Personal data related to audits will be stored in the document management tool(s) for 5 years after finalisation of the final audit report.

Personal data related to the assessment of personal data breaches are stored in the document management tool(s) for 10 years after finalisation of the data breach report.

Personal data processed to provide support and/or opinions, or recommendations in relation to Article 49 DPR (request for review by the delegated controller), Article 50 DPR (legal redress) and Article 51 DPR (incidental data protection request during internal appeal proceedings – only relevant for EPO staff) will be stored in the document management tool(s) for 10 years after finalisation of the opinion.

The retention period of the personal data contained in the documents received by the DPO, in the performance of its tasks, is also defined in the records of operational processes supported by those documents.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Personal data related to records inserted in the EPO Data Protection Register will be stored as long as the processing is operational.

After that date the record will be deleted from the Register but archived the period of 5 years for reasons of possible legal appeal procedures.

Personal data related to consultations, complaints, requests from the data subjects and data

protection audits will be archived in the document management tool for the period of 5 years.

Personal data related to complaints filed with the DPB are to be kept for:
i. a maximum of 5 years after the closure for inadmissible complaints
ii. a maximum of 10 years after closure of an admissible complaint.

Personal data related to the personal data breaches are to be kept for 10 years after closure of the case.

The retention period of the personal data contained in the documents is also defined in the records of the operational processes supported by those documents.

The records' retention schedule also indicates the subsequent actions at the end of the administrative retention period on the basis of the potential historical value of documents and files. These actions include elimination of certain data, sampling or selection and long-term preservation of the documents and cases identified as archives.

Data subjects and categories of personal data

Contractors

Applications' Log	
SAP Logs	
Sensory and Electronic Information	
Audio Information	Electronic Information
Thermal Information	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name

Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
General	
Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	Nomination justificative
User association	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Previous Residence Address
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Correspondence	

Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
File data (name, size and/or hash)	Ports
Registry data	Running Processes
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	Operating System Version
Smart Card Number	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Appeals Records Information	Assessment and legal opinions
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Disciplinary Action	Duration of employment

End Date	End Date and Reason for Termination
EPO access badge number	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Language preference (of communication)
Line Reporting Manager	Membership in a EPO Staff Committee
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Record of Maternity Leave	Room Number
Salary	Start Date
Weight	
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Political Affiliation and Activities	Professional Memberships
Qualifications Certifications	Trade Union Membership

Examination content data	
Examination marks	Examination result
Financial	
Bank Account Information	Bank Account Number
Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
User Account Information	
Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	
Driving Licence Number	National Identification Number
National Identity Card Details	Passport Number
Social Security Number	

Employees

Applications' Log	
SAP Logs	
Sensory and Electronic Information	
Audio Information	Electronic Information
Thermal Information	Time stamps from their access to the buildings

Visual Information	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
General	
Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	Nomination justificative
Personal Information in SAP	Sensitive Personal Data in SAP
Special Categories of Data in SAP	User association
Workplace Welfare	
Records of Personal Properties	
Contact Information	

Contact Details	Country
Emergency Contact Details	Home Address
Home Leave Address	Mobile Phone Number
Personal Email	Phone Numbers
Previous Residence Address	Teleworking address
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
Diagnostic tools’ results	IDP
Instructor related data	Learning external events
Learning history	Learning plan
Ratings	Social learning inputs
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
File data (name, size and/or hash)	Ports
Registry data	Running Processes
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	Operating System Version
Smart Card Number	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	

Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Appeals Records Information	Assessment and legal opinions
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Disciplinary Action	Duration of employment
End Date	End Date and Reason for Termination
EPO access badge number	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Group	Job Title Role
Language preference (of communication)	Line Reporting Manager
Membership in a EPO Staff Committee	Military Status
Office Location	Performance Rating
Personnel Number	Previous Work History
Record of Absence/Time Tracking/Annual Leave	Record of Maternity Leave
Rewards history	Room Number
Salary	Start Date
Weight	
Unknown	

EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Political Affiliation and Activities	Professional Memberships
Qualifications Certifications	Trade Union Membership
Examination content data	
Examination marks	Examination result
Family Information	
Child’s Level/Year of Studies	Child’s School Enrolment Date Start
Children's Names	Child's birthday
Composition of the family (number of dependent children/persons)	Parents' Names
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number
Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans

Insurance Information	Routing Number
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
User Account Information	
Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	
Car registration documents	Driving Licence Number
National Identification Number	National Identity Card Details
Passport Number	Social Security Number

Externals

Applications' Log	
SAP Logs	
Sensory and Electronic Information	
Audio Information	Electronic Information
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name

Gender	Surname
Nationality	Picture
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
General	
Any other information	Input provided during the deliberation and decision-making process
Nomination justificative	User association
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Ratings
Social learning inputs	
European Patent Register Data	
Address	Data provided by the data subjects
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
System Logs	

File data (name, size and/or hash)	Ports
Registry data	Running Processes
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	Operating System Version
Smart Card Number	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Facial Recognition	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Employment Information	
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	Duration of employment
End Date	EPO access badge number
Hours of Work	Job Title Role
Language preference (of communication)	Membership in a EPO Staff Committee
Office Location	Previous Work History
Record of Maternity Leave	
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Network/application Interaction Data	
Session content	Session details
Session metadata	

Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Political Affiliation and Activities	Professional Memberships
Qualifications Certifications	
Examination content data	
Examination marks	Examination result
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
User Account Information	
Account Age	Account Number
Account Password	
Government Identifiers	
National Identity Card Details	Passport Number

Former Employees

Applications' Log	
SAP Logs	
Sensory and Electronic Information	
Audio Information	Electronic Information

Thermal Information	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
General	
Any other information	Input provided during the deliberation and decision-making process
Nomination justificative	Personal Information in SAP
Sensitive Personal Data in SAP	Special Categories of Data in SAP
User association	
Workplace Welfare	
Records of Personal Properties	

Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Home Leave Address	Mobile Phone Number
Personal Email	Phone Numbers
Previous Residence Address	Teleworking address
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
File data (name, size and/or hash)	Ports
Registry data	Running Processes
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	Operating System Version
Smart Card Number	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	

Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	Disciplinary Action
Duration of employment	End Date
End Date and Reason for Termination	EPO access badge number
Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Group
Job Title Role	Language preference (of communication)
Line Reporting Manager	Membership in a EPO Staff Committee
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Record of Maternity Leave	Rewards history
Salary	Start Date
Weight	
Unknown	
EPO badge validity	Identification of which membership is envisaged

Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Political Affiliation and Activities	Professional Memberships
Qualifications Certifications	Trade Union Membership
Examination content data	
Examination marks	Examination result
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number
Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address

Network Interaction History	Website History
User Account Information	
Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	
Driving Licence Number	National Identification Number
National Identity Card Details	Passport Number
Social Security Number	

Prospective Employees

Applications' Log	
SAP Logs	
Sensory and Electronic Information	
Time stamps from their access to the buildings	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Religion/Religious Beliefs	Signature
Education & Skills	

Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
General	
Any other information	Input provided during the deliberation and decision-making process
Nomination justificative	User association
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
System Logs	
File data (name, size and/or hash)	Ports
Registry data	Running Processes
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Operating System Version	Workstation Serial Number

Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Department name and/or number	Duration of employment
End Date	End Date and Reason for Termination
EPO access badge number	Grade
Job Application Details	Job Group
Job Title Role	Language preference (of communication)
Line Reporting Manager	Membership in a EPO Staff Committee
Military Status	Office Location
Performance Rating	Previous Work History
Record of Maternity Leave	Rewards history
Salary	Start Date
Weight	
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	

Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Political Affiliation and Activities	Professional Memberships
Qualifications Certifications	
Financial	
Fund Reservation Requests	Information on home loans
Examination content data	
Examination marks	Examination result
Browsing Information	
Browser type	
User Account Information	
Account Age	Account Number
Account Password	Password
Government Identifiers	
National Identity Card Details	Passport Number

Recipient of the personal data

Recipients of the data Where strictly necessary to perform its tasks, personal data may be disclosed on a need-to-know basis to the staff working in the DPO, to the relevant controller, the delegated controller(s), the DPLs and to any other authorised staff. Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

Personal data processed in the DP Tool may be disclosed to a third-party service provider for maintenance and support purposes of the DP tool.

Personal data may be disclosed to the Data Protection Board when the DPO's support is requested.

In addition:

- in the case of data subject (internal or external) enquiries, personal data may be disclosed to the delegated controllers responsible for the processing operation related to the enquiry. Strictly necessary personal data may be shared with other units (such as a technical team or human resources) as necessary to collect and compile relevant information to respond to the enquiry
- in the case of data breaches, personal data may be disclosed to the President of the Office, the delegated controller, the processor and authorised staff as necessary to handle the breach
- in the case of an investigation under Article 43(1)(d) and (2) DPR, personal data may be disclosed to the person who commissioned the data protection investigation and/or the President of the Office, the delegated controller, the processor or the body set up under the legal provisions of the European Patent Organisation
- in the case of an audit under Article 43(1)(d), personal data may be disclosed to the President of the Office, the delegated controller (auditee) and the processor
- in the case of an opinion requested from the DPO under Article 49(2) DPR, personal data may be disclosed to the delegated controller who received the request for review
- in the case of an opinion requested from the DPO under Article 51 DPR, personal data may be disclosed to the body under the Service Regulations advising the appointing authority and to the appointing authority
- in the context of co-operation with external and internal stakeholders, personal data may be disclosed to authorised staff members of the DPO, the President of the Office or the relevant delegated controller.

Purpose of sharing - to perform the DPO's tasks and duties
- to provide support to the DPB upon request
- to co-operate with external and internal stakeholders

Depending on the case, personal data might be disclosed to different recipients:

- in the case of an investigation according to Articles 43 (1)(d) and 43(2) DPR, personal data might be disclosed to the person who commissioned the data protection investigation or the President, the delegated controller, the processor or the body set up under the legal provisions of the European Patent Organisation;
- in the case of an opinion requested to the DPO according to Article 49(2) DPR, personal data might be disclosed to the delegated controller that received the request for review;
- in the case of an opinion requested to the DPO according to Article 51 DPR, personal data may be disclosed to the body under the Service Regulations advising the appointing authority and the appointing authority.

In the context of data protection audit, personal data (such as performance indicators, privacy metrics or DPO audit reports and follow up reports), might be disclosed to the President and the Presidential Office. Audit reports and follow up reports might be published on the DPO corner on Intranet.

Personal data might be disclosed to the DPB when the support of the DPO is requested.

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OneTrust - United States, OpenText - United States, TRE Thomson Reuters - Luxembourg

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses, A derogation in accordance with Art. 10 DPR

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet
http://documents.epo.org/projects/babylon/eponet.nsf/0/F787612FB623B8BAC1258821003526E0/$FILE/data_protection_statement_on_the_processing_of_personal_data_en.pdf

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 21

Name Collection and management of contact lists of Brussels' stakeholders

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 01 - Chief of Staff, President`s Office

Entity Name - Processor (Entities)

Description of the processing

Description The source of the personal data of Brussels' stakeholders is either publicly available information or information retrieved through personal contact with organisations of interest. The data thus collected is entered in the delegated controller's contacts data base. The personal data from these lists is used for invitations to EPO events or information on EPO activities.

As for the destruction of the data, we update our database regularly considering that Brussels based stakeholders usually remain in post for a period of 3 to 5 years.

Data Retention The personal data of the data subjects concerned is kept in the lists as long as they remain Brussels IP stakeholders as defined above. Once the data subjects are not fulfilling these conditions anymore, the personal data is deleted

Purpose of Processing Personal data is processed for the purpose of developing and maintaining a network of formal and informal contacts with Brussels' key players such as the EU Institutions, relevant stakeholders (industry federations, NGOs, law firms, other public entities etc).

Data subjects and categories of personal data

Externals

Sensory and Electronic Information	
Electronic Information	
Contact Information	

Contact Details	Home Address
Personal Email	Phone Numbers
Professional Experience & Affiliations	
Political Affiliation and Activities	Professional Memberships
Personal Identification	
First Name	Full Name
Gender	Surname
Nationality	

Recipient of the personal data

Recipients of the data The EPO Communication Department will have access to limited information of the data subjects stored on the contacts database (name, first name, organisation, position, where applicable Directorate/Department and responsibilities)

Purpose of sharing Need to know basis (to inform data subject on the launch of EPO studies or any EPO activities)

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 22

Name Internal audit

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 041 - Internal Audit and Professional Standards - Internal Audit

Entity Name - Processor (Entities) DG0 - 05 - Administration of Reserve Funds, DG4 - 41 - Finance, DG4 - 42 - People, DG4 - 421 - Talent Management, DG4 - 422 - HR Customer Engagement, DG4 - 423 - HR Essential Services, DG4 - 43 - Welfare & Remuneration, DG4 - 44 - General Administration, DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

Consulting Auditing Firms

External processors	
Name Consulting Auditing Firms	

Description of the processing

Description Internal Audit processes personal data to achieve its mission (namely to enhance and protect organisational value by providing risk-based and objective assurance, advice and insight). Internal Audit interviews staff responsible for the audited operations, carries out surveys, analyses documentation and data in information systems. The Internal Audit activities do not typically target natural persons as such. Nevertheless, personal data are inevitably processed during the course of Internal Audit activities (i.e. for the internal audit's planning, fieldwork and follow-up).
As a general rule, the audit reports submitted to the President (RFPSS SB) are anonymised; therefore, no data sharing has to be considered.

Purpose of Processing Planning and conducting internal audits, issuing internal audit reports to the President (or the RFPSS Supervisory Board) and following up on the implementation of recommendations.

Data Retention The retention period for internal audit working papers is 10 years after the closure of the internal audit cycle.

Data subjects and categories of personal data

Contractors

Contact Information	
Contact Details	Home Address
Phone Numbers	Previous Residence Address
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Financial	
Bonus Payments	Compensation Data
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Background Checks	
Criminal History	Criminal Records
Reference or Background Checks	
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Disciplinary Action	End Date

End Date and Reason for Termination	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Line Reporting Manager
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Salary	Start Date
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Height	Surname
Marital Status	Nationality
Signature	
User Account Information	
User ID	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages

Employees

Contact Information	
Contact Details	Home Address
Home Leave Address	Personal Email
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data

IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Financial	
Bonus Payments	Compensation Data
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Background Checks	
Criminal History	Criminal Records
Reference or Background Checks	
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Disciplinary Action	End Date
End Date and Reason for Termination	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Line Reporting Manager
Military Status	Office Location

Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Salary	Start Date
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Marital Status
Nationality	Signature
User Account Information	
User ID	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages

Externals

Contact Information	
Phone Numbers	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	

Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
End Date	Hours of Work
Job Title Role	Office Location
Previous Work History	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Nationality
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages

Former Employees

Contact Information	
Contact Details	Home Address
Home Leave Address	Phone Numbers
Previous Residence Address	Teleworking address
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications

Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Financial	
Bonus Payments	Compensation Data
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Background Checks	
Criminal History	Criminal Records
Reference or Background Checks	
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Disciplinary Action	End Date
End Date and Reason for Termination	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Line Reporting Manager
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Salary	Start Date
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name

Full Name	Gender
Surname	Marital Status
Nationality	Signature
User Account Information	
User ID	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages

Recipient of the personal data

Recipients of the data Internal Audit members, any person duly assigned by the Director of Internal Audit and the Principal Director Internal Audit and Professional Standards.

Internal audit reports are submitted to the President (or the RFPSS Supervisory Board) for decision on recommendations. The internal audit reports are forwarded to the management of the audited units and a copy is provided to the Board of Auditors.

As a general rule, the information presented in the internal audit reports shall be anonymised.

Purpose of sharing planning and conducting internal audits, following up on the implementation of recommendations

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 26

Name Selection of members of SACEPO (Standing Advisory Committee before the EPO) and its working parties

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft	

Any participant from outside the EEA

External processors	
Name Any participant from outside the EEA	

Description of the processing

Description The SACEPO and its specialist SACEPO Working Parties (Quality, Rules, Guidelines, Patent Information and E-Patent Process) are composed of user representatives appointed by the President of the Office. Some of them are proposed by users associations, the remainder are directly identified and appointed by the Office.

The Sacepo secretariat collects the information provided by the IP stakeholders/associations and/or by the candidates themselves. It prepares the file for the final part of the deliberation and decision-making process. This involves a first evaluation of the suitability of the candidates also with regard to the need to have a sufficiently balanced composition of SACEPO and each of its working parties. This is related to the purpose of having a balanced representativeness of the users community (e.g. technical fields, SMEs versus big companies) and of the society (e.g. genders, nationality).

The candidates finally appointed by the President are informed via an official letter. Previous members who are not re-appointed are informed via email. Other unsuccessful candidates are informed indirectly, as the list of newly appointed SACEPO members is published on the SACEPO webpages of the EPO's Internet. The SACEPO webpages can be found here. https://www.epo.org/about-us/services-and-activities/Consultingourusers/sacepo/members.html

SACEPO secretariat stores the electronic information received via email in its dedicated SACEPO mailbox. Paper files might also be prepared, in which case they are stored in the archive room(s) of the SACEPO secretariat.

he personal data of all the successful and unsuccessful candidates is kept by the SACEPO Secretariat at least until the next selection round is over.

Data Retention

Personal data processed are stored for the period of time necessary to achieve the purpose for which they have been processed.

Purpose of Processing Use the data of appointed members for the organisation of the SACEPO meetings, - Selection of members of SACEPO and its specialist SACEPO Working Parties, in such a way that the user groups are as representative as possible of the stakeholder groups which the Office would like to consult and of society as a whole. - publication of the appointments. - providing the SACEPO secretariat with a pool of potential candidates for next selection rounds.

Data subjects and categories of personal data

Externals

General	
User association	

Contact Information	
Contact Details	Personal Email
Phone Numbers	Working email address
Professional Experience & Affiliations	
Affiliation	CV
Professional Memberships	Qualifications Certifications
Correspondence	
Additional Information which might be provided in the course of exchanges	
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Previous Work History	
Personal Identification	
First Name	Full Name
Gender	Surname
Nationality	
Education & Skills	
Education and Training History	Educational Degrees
Languages	

Employees

General	
Input provided during the deliberation and decision-making process	
Contact Information	
Contact Details	Phone Numbers
Employment Information	
Business Unit Division	Department name and/or number
Job Title Role	Office Location

Personnel Number	Room Number
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data (1) EPO hierarchy

(2) Other EPO employees (not hierarchy)

(3) Internal stakeholders of SACEPO

(4) The public

Purpose of sharing (1) EPO hierarchy involved in the internal deliberation and decision-making process.

(2) Office’s employees involved in the selection process (on a need-to-know basis).

(3) Internal stakeholders of SACEPO might be consulted, in which case only the part of the personal data of the candidates necessary for this consultation is shared (usually name/contact details and specific criteria discussed)

(4) The public, as the list of newly appointed SACEPO members is published on the SACEPO webpages of the EPO’s Internet

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 33

Name Email newsletters and alerts

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 02 - Communication

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT, DG5 - 51 - Cooperation and Patent Academy, DG5 - 54 - Patent Knowledge

External processors

Poppulo

External processors	
Name Poppulo	

Description of the processing

Description There is a single registration form for subscribing to EPO newsletters. In such registration form, there are five optional sections, which, if selected, will be sent to the subscriber in addition to the general newsletter, which is sent to all subscribers to the newsletter.
PDComm has access to all the lists of subscribers to the newsletter and is in charge of sending the general newsletter.

In addition, the data subject can also subscribe to other alerts the EPO provides:

 the Official Journal
 Learning alerts
 Press alerts
 User consultations
 EIA newsletter
 Online services

To collect the data for statistics and send the email newsletters and alerts, the departments use Poppulo's Newsweaver tool. Some departments have one or several Poppulo accounts.

The user can unsubscribe at any time by clicking on the link provided in the footer of the email alert or the newsletter. To change subscription preferences, the user is informed in the Newsletter FAQs that, among other information, he/she has to complete a new registration form with the new preferences to update the profile automatically.

If the user has a problem with the unsubscribe procedure or wishes to make any request, he/she can send an email to website@epo.org

When the user uses the email website@epo.org, Poppulo is not involved, as this is a regular internal EPO email inbox. In this case, when the user asks for rectification or deletion of your data, the EPO replies with an explanation about how they can change their preferences via the tool.

Data Retention We will collect and update the data until the user decides to unsubscribe to the newsletter. If the user only unsubscribes from one section, we will continue processing the data for the rest of the newsletters.

Data is also deleted automatically if an email publication is stopped.

Users can unsubscribe at any time by clicking on the link provided in the "Useful links" section of the newsletter received. They can also send an email to website with the words "Unsubscribe newsletter" in the subject line and the EPO will then provide further instructions.

Purpose of Processing informing our subscribers about news and information on European patent law and procedure, patent information and searching, and other EPO services, such as events.

Data subjects and categories of personal data

Externals

Contact Information

Contact Details	Home Address
Personal Email	Phone Numbers
Employment Information	
Job Title Role	Office Location
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data Personal data, depending on its type and the purpose of its processing, is made accessible only on a need-to-know basis to EPO staff members and the external providers and their sub-contractors.

Different business units at the EPO as mentioned above, will have access to the information stored on the contact details database on a need-to-know basis. Some users in PD Comm, have access to some subscribers Database (as well as some user in Patent Info, Academy and Patent Administration). In addition, a CM administrator selected in the Principal Directorate Communication and a DC administrator in BIT have an administrator account and can access all subaccounts and the database of data subjects.

In each sub-account, Poppulo has a subscriber Database. Each subscriber is tagged (by interest, preferred language, preferred email format or country) which allows them to search users based on tags and add them to an audience. The newsletter is sent to users of Audiences.

Purpose of sharing Personal data, depending on its type and the purpose of its processing, is made accessible only on a need-to-know basis to EPO staff members and the external providers and their sub-contractors.

Different business units at the EPO as mentioned above, will have access to the information stored on the contact details database on a need-to-know basis. Some users in PD Comm, have access to some subscribers Database (as well as some user in Patent Info, Academy and Patent Administration). In addition, a CM administrator selected in the Principal Directorate Communication and a DC administrator in BIT have an administrator account and can access all subaccounts and the database of data subjects.

In each sub-account, Poppulo has a subscriber Database. Each subscriber is tagged (by interest, preferred language, preferred email format or country) which allows them to search users based on tags and add them to an audience. The newsletter is sent to users of Audiences.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet
Under preparation

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 38

Name Operational reporting information used internally on the Tableau / BI4you platform

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 41 - Finance, DG4 - 47 - Procurement and Vendor Management

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

Description of the processing

Description On the BI4YOU platform, the data is reported based on SAP tables loaded and transformed in various systems. The access to the tables is reserved to a limited number of Power Users and the roles to view the SAP tables at the source is given following a standardized process managed by BIT (BOSS team).
Following a formal request for extraction by the power user, certain SAP tables and reports are made available for the reporting tools. Here, several tables are joined to produce the final report. Access to the aggregated reports is given to the end users after they are added to reporting groups in Bi4YOU or to specific dashboards.
Access to tables within the reporting platform is given to a limited number of users, after it is cross-checked with the SAP roles.
The reports are available on the platform until they become obsolete (i.e. process changes) or no longer viewed by the users.
Once created, dashboards are automatically updated with the latest data or when other requirements are presented to the Power user.
Exceptionally, when an automatic extraction is not possible, a manual download to an excel is performed for further analysis.

Purpose of Processing • Calculate cycle times per entry involving multiple approvals • Escalations in case of non-compliance (reminders), Documenting the author of a respective entry, Aggregate entries per team, site, groups

Data Retention For Finance and Procurement the report's retention period depends on the time the process is active and it is based on the data retention policies of the underlying tools (SAP) The reports are available on the platform until they become obsolete (i.e. process changes) or no longer viewed by the users.

Once created, dashboards are automatically updated with the latest data or when other requirements are presented to the Power user.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Phone Numbers
Financial	
Bank Account Information	Bank Account Number
Employment Information	
Business Unit Division	Company Entity
Contract Type	Job Title Role
Office Location	
Personal Identification	
First Name	Full Name
Surname	Signature

Contractors

Employment Information	
Business Unit Division	Job Title Role
Personnel Number	
Personal Identification	
First Name	Surname
User Account Information	
User ID	

Employees

Employment Information

Business Unit Division	Job Title Role
Personnel Number	
Personal Identification	
First Name	Surname
User Account Information	
User ID	

Recipient of the personal data

Recipients of the data Recipients within the controller (EPO) including individuals from different operational units across the Office, as is required to fulfil their operational responsibilities.

Purpose of sharing recipients within the controller (EPO) including individuals from different operational units across the Office, as is required to fulfil their operational responsibilities.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 39

Name Bulk data Patent Knowledge products delivery

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 54 - Patent Knowledge

Entity Name - Processor (Entities) DG4 - 44 - General Administration, DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

INIT

External processors	
Name INIT	

Description of the processing

Description The European Patent Office (EPO) distributes European Patent Grant procedure related data and world-wide patent data in the form of bulk datasets which can be downloaded by users from the EPO Bulk Data service. Some of the services are based on user subscription.

Subscriber and subscription information is processed by the Customer Support Team (CSC) within the EPO and subscriber data corresponding to the bulk data subscriptions are sent to the bulk data hosting provider (an external service company). This subscription information processing is described in the scope of the record “Patent Knowledge Web Shop”.

Based on the external users’ subscription information, the hosting provider manages the access to the patent data sets. EPO staff may also access and manage the subscriber data managed by the hosting provider in specific support cases.

Personal data is also used for analytics and service delivery as well as the to provide support and distribute event information to users.

In special cases delivery may involve the use of post services.

Data Retention User data is retained for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore (e.g. cancellation of a subscription).
Technical service access data can be retained for up to 7 years in order to analyse usage patterns.
Information contained in the patent records is public data which is never deleted.

Purpose of Processing Distribute support and event information to users., Delivery of Bulk Data products to users., Analytics and service delivery

Data subjects and categories of personal data

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers
Working email address	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Employment Information	
Company Entity	
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
Personal Identification	
First Name	Full Name
Gender	Surname
User Account Information	
Account Password	User ID

Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Browsing Information	
IP Address	
User Account Information	
Password	User ID

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Knowledge, Finance, BIT, DG1, PD44 General Administration and senior EPO management (CILO, VP5 Office, MAC, President's Office).

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer The service is intended to deliver patent data to world-wide users.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet Will be made available after DPO review of this record, and include link to: ....

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 40

Name Patent Knowledge News

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 54 - Patent Knowledge

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description The EPO provides news content by various authors for inclusion in the patent knowledge on-line news (PKN) service as part of the EPO web site.

External and internal users access PKN via the standard EPO web site protocols and interact with the PKN service via a functional email account for the EPO's Patent Knowledge News, which is setup in order to:

- Facilitate communication between the EPO staff in charge of Patent Knowledge News and the users/readers/contributors.

- Facilitate information exchange (receiving questions, comments, suggestions, quiz results, enquiries and providing feedback) and other user engagement activities.

The EPO will answer the readers' questions directly or forward the inquiries to internal and/or external experts who would then respond to the reader.

To carry out the tasks and activities described, the Office uses Microsoft Office 365 applications.

Data Retention The retention policy is set to maximum 7 years. If considered appropriate, it is also deleted if it can reasonably be expected that there is no operational need anymore.

Microsoft Outlook retains personal data as long as it is necessary for the purposes for which personal data was collected. After expiration or termination of the Contract, Microsoft stores personal data for 90 days to allow the EPO to extract the data. After the 90-day retention period ends, Microsoft will disable EPO's account and delete the personal data within an additional 90 days, unless Microsoft is permitted or required by applicable law to retain such data.

Purpose of Processing Provide online access to Patent Knowledge News, Facilitate information exchange (receiving questions, comments, suggestions, enquiries and providing feedback) and other user engagement activities., Facilitate communication between the EPO staff in charge of Patent Knowledge News and the users/readers/contributors.

Data subjects and categories of personal data

Employees

Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers

Externals

Contact Information	
Contact Details	Personal Email
Phone Numbers	
Correspondence	

Personal information provided voluntarily

Recipient of the personal data

Recipients of the data The personal data are disclosed on a need-to-know basis to the EPO staff involved in Patent Knowledge News related activities.

Personal data might be disclosed to Microsoft for maintenance, support and security purposes, as well as BIT and Microsoft staff involved in the data processing necessary to provide the Microsoft services.

Personal data will be shared with authorised persons responsible for the corresponding processing operation. They will not be used for any other purposes or disclosed to any other recipients.

Purpose of sharing - EPO staff: deliver service to the user by management and publication of Patent Knowledge News.
- Microsoft and BIT: provide the Microsoft services, as well as for maintenance, support and security purposes.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Security purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet
https://www.epo.org/about-us/office/data-protection-and-privacy/epo-patent-knowledge-news.html

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 41

Name European Publication Server

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 54 - Patent Knowledge

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

N.A.

External processors	
Name N.A.	

Luminess

External processors	
Name Luminess	

Description of the processing

Description The European Patent Office (EPO) publishes patent documents by decision of the President of the EPO published in the EPO Official Journal of February 2005, and the European Publication Server has been the sole legally authoritative publication medium for European A and B documents since 1 April 2005. All documents are available for public access from any location free of charge on their day of publication.

Patent publication data is prepared during the Patent Grant procedure, and subsequently distributed via the European Publication Server.

In addition to the above mentioned “content” processing, additional processing is undertaken in order to provide service usage analytics and ensure correct service functioning.

Data Retention The EP publications are public data, and therefore the data is not deleted. User data is retained for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore.

Purpose of Processing Analytics, and ensuring correct service functioning., Online distribution of published European Patent documents.

Data subjects and categories of personal data

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History

Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO and external contractors: Patent Knowledge, BIT, DG1 and senior EPO management (CILO, VP5 Office, President Office, CGS, MAC), external contractors working for the aforementioned areas of the EPO may access

Purpose of sharing Publication is done in accordance with the provisions of the European Patent Convention.
Administrative information is shared to ensure correct functioning of the service and to facilitate usage analysis.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation The published data are publicly accessible.

Transfer mechanism(s) A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Luminess - France

Reasons for the transfer The patent record content is made available to anyone world-wide., Publication is done in accordance with the provisions of the European Patent Convention.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet Will be made available after DPO review of this record, and include link to: ....

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 42

Name PISE Services

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 54 - Patent Knowledge

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

Luminess

External processors	
Name Luminess, Luminess	

Description of the processing

Description The European Patent Office (EPO) distributes Patent Information Services for Experts (PISE) to users. These services include:
- EP FULL TEXT
- EP BULLETIN SEARCH
- GPI
- PATSTAT hosted

These are web based services, and some areas require user registration which is linked to an integrated Internet Access Control based upon the user credentials.

The patent procedure records may also contain personal information as an intrinsic part of the subject matter treated in the record (inventors, applicants, EPO officers etc).

Purpose of Processing Delivery of PISE services to users.

Data Retention User data is kept for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore (e.g. cancellation of a subscription).
Technical service access data can be kept for up to 7 years in order to analyse usage patterns.
Information contained in the patent records is public data which is never deleted.

Data subjects and categories of personal data

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Contact Details	Country
Personal Email	Working email address
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Employment Information	
Company Entity	
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
Personal Identification	
First Name	Full Name
Gender	Surname
User Account Information	
Account Password	

Employees

Patent Process Related Data

Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world wide. Personal data of users may be shared with authorised persons responsible for the corresponding processing operations and any other EPO staff members who need to have access to the data only on a need to know basis.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation The published data are publicly accessible.

Transfer mechanism(s) A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Luminess - France

Reasons for the transfer The patent related content is made available to anyone world-wide.

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet Will be published under this link: ....

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 43

Name EPO hosted PK services

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 54 - Patent Knowledge

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

Not Applicable.

External processors	
Name Not Applicable.	

Description of the processing

Description The European Patent Office (EPO) provides public access to the Espacenet and EP Register in order to facilitate search, access, retrieval, and analysis of patent data. Users may additionally subscribe to customised services such as alerts.

The data is provided from systems which support the Patent Grant Procedure, and diverse procedural, legal status, post grant, reference, and other data collections of the EPO. The data relates to procedures under the European Patent Convention (EPC) and world-wide jurisdictions.

EP Register includes an "Alert" service for which users may register.

Usage analytics related data are processed in order to support the efficient delivery of the services.

Purpose of Processing Usage analytics and ensuring correct service functioning, Provide user access to Patent Knowledge services hosted by EPO

Data Retention User data is retained for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore (e.g. cancellation of a subscription).
Technical service access data can be retained for up to 7 years in order to analyse usage patterns.
Information contained in the patent records is public data which is never deleted.

Data subjects and categories of personal data

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Personal Email	Working email address
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Employment Information	
Company Entity	Language preference (of communication)
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
Personal Identification	
First Name	Full Name
Gender	Surname
User Account Information	
User ID	

Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

User Account Information	
Password	User ID

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data Personal data will only be shared on a need to know basis. Namely, the data is shared with the following recipients:

General public: patent information forming part of the public patent record

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Knowledge, BIT, DG1 and senior EPO management (CILO, VP5 Office, President Office, CGS, MAC, PD Communication,).

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation The published data are publicly accessible.

Transfer mechanism(s) A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer The patent related content is intended to be made available to anyone world-wide.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet Will be made available after DPO review of this record, and include link to: ....

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 45

Name PK Web Shop

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 54 - Patent Knowledge

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 44 - General Administration, DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

SAP

External processors	
Name SAP	

Commerzbank | European Patent Office | Unknown

External processors	
Name Commerzbank | European Patent Office | Unknown	

Description of the processing

Description The EPO online shop is an web based platform where individuals can order EPO Patent Knowledge related products and services where Patent Knowledge is understood to be knowledge that serves to foster the effective use and dissemination of patent data.

Personal data are processed and used as described below:

• Personal data is collected and processed for the purpose of processing orders and promotion and marketing activities of the EPO.

• The personal data of EPO online shop customers is collected during user account registration process. Customers connect to the EPO online shop area of the EPO website to register and/or maintain their account information. An account is required before using the EPO online shop to place orders.

• The personal data is stored in the back-end system of the EPO online shop and the EPO's SAP back-end system. The list of Patent Knowledge related products and services is dynamic, and the current status can be found in the EPO website. In certain cases, information in the back-end system may be manually entered by EPO Patent Knowledge staff.

• When needed to handle order processing related issues, personal data are used for identifying the user. To resolve the issue, further personal data provided by the user, might be used.

• To carry out promotion and marketing of EPO products and services. The users may be contacted via the communication channel indicated during the registration process.

• To carry out payment transaction processing for invoiceable products and services, necessary personal data are processed by the relevant EPO departments. The invoicing is undertaken by the Customer Service Centre (CSC) within the Patent Knowledge business area of the EPO, and is based on the information mentioned above. Payment processing in undertaken by the Finance department of the EPO.

• For IT support and maintenance, product and service delivery, improvement of the overall service and user experience.

Users may terminate subscriptions by contacting the EPO in accordance with the terms for the relevant products and services, and information will be retained in accordance with this record.

The tools and platforms are integrated across a range of domains, and encompass activities and products / services offered falling under the responsibilities multiple internal and processors as further elaborated in this record.

Purpose of Processing Provide a Webshop frontend for users, order processing, invoicing, user account registration and subscription management., IT support, delivery and maintenance., Service improvement., Payment transaction processing., Ad-hoc contact with users and marketing.

Data Retention User data is retained for to 7 years. If considered appropriate, data is deleted if it can reasonably be expected that there is no operational need anymore.

Financial data is retained for 10 years, in line with the EPO financial regulations.

Data subjects and categories of personal data

Externals

General	
Any other information	
Contact Information	
Contact Details	Country
Home Address	Personal Email
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
VAT ID Number	
Employment Information	
Company Entity	
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
Personal Identification	
First Name	Full Name
Gender	Surname

Nationality	Signature
Education & Skills	
Languages	
User Account Information	
Account Age	Account Number
Account Password	

Recipient of the personal data

Recipients of the data The patent record content can be made available to Webshop customer ordering a relevant product. These customers may be world wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Knowledge, BIT, Finance, senior EPO management (CILO, VP1 Office, VP4 Office, VP5 Office, President's Office, CGS, MAC) as well as with external contractors providing related processing.

Purpose of sharing

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors) SAP - United States

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet To be completed later

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 47

Name PATLIB

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 54 - Patent Knowledge

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

SAP

External processors	
Name SAP	

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description The "PATLIB centres", standing for PATent LIBrary, provide local access to patent information and related issues. They are familiar with the local industrial, economic and business landscape, and provide valuable services to entrepreneurs, SMEs, private inventors and students.

The EPO co-ordinates the PATLIB network.

Personal data are processed only for the purpose of carrying out the administration, collaboration and communication involving the PATLIB centres.

PATLIB related processing:
- Network
- Directory of PATLIB Centres
- Collaboration with PATLIB Network staff
- Collaboration with third parties
- Administration
- Committee
- Ad hoc meetings
- News
- Conference / Other PATLIB network related events
- Trainings

Data Retention Personal data will be kept for as long as the person is a member of the network and three years thereafter.

Purpose of Processing Email Communication and User Questionnaire Management, Identifying participants and contributors to PATLIB activities, Information exchange on events within the PATLIB network events calendar, Administration of PATLIB network, Inviting data subjects with certain recorded skills to collaborate within the PATLIB network as experts, speakers, consultants, etc., Communicating within the PATLIB network, Keeping an online directory of PATLIB centres and experts; the directory is available to the public to find IP specific support and contains contact details of the PATLIB centres and their experts. Through to self-administration, the centres decide on type and amount of disclosed details, Document exchange within the PATLIB network, Providing data subjects with information about the PATLIB activities by means of a regular email, Keeping a record of data subjects' participation in activities organised in the PATLIB network, the business cases submitted and any feedback received., Providing data subjects with invitations to PATLIB and other IP-related EPO meetings, events and trainings

Data subjects and categories of personal data

Externals

Social	
Social Media Account	Social Media Contact
Health Data	
Health Data	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Personal Email
Phone Numbers	Working email address
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number

Insurance Information	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
End Date	Hours of Work
Job Title Role	Office Location
Previous Work History	
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Nationality
Signature	
User Account Information	
Account Age	Account Number
Account Password	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Government Identifiers	

National Identity Card Details	Passport Number

Employees

Social	
Social Media Account	Social Media Contact
Social Media History	
Health Data	
Health Data	
Contact Information	
Contact Details	Emergency Contact Details
Personal Email	Phone Numbers
Working email address	
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	
Business Unit Division	Line Reporting Manager
Office Location	Personnel Number
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
Personal Identification	
Age	Date of Birth

Disability or Specific Condition	First Name
Full Name	Gender
Surname	Nationality
Signature	
Education & Skills	
Education and Training History	Languages
User Account Information	
Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	
Passport Number	

Contractors

Health Data	
Health Data	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Personal Email
Phone Numbers	Previous Residence Address
Teleworking address	Working email address
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
Routing Number	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber

Recipient of the personal data

Recipients of the data The personal data are disclosed on a need-to-know basis to the following recipients:
• Participants in the PATLIB network and activities
• EPO staff members and non-EPO staff working on behalf of the EPO undertaking relevant duties
• Staff of national patent offices

The personal data are not disclosed to any other recipient.

Furthermore, the part of personal data disclosed in the online directory is available to the public without restriction.
The PATLIB Centre is responsible for the accuracy of its own data within the PATLIB directory.
Any third-party is directly responsible for misusing the publicly accessible data within the PATLIB directory.

Personal data might be disclosed to third-party service providers for maintenance and support purposes.

Personal data will only be shared with authorised persons responsible for the corresponding processing operations and are not used for any other purposes or disclosed to any other recipients.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation National Patent Offices

Transfer mechanism(s) The recipient provided appropriate safeguards, A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, SAP - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities, Public Authorities/Government Bodies, Further development of the PATLIB Network, To facilitate the execution of PATLIB related activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet
https://www.epo.org/about-us/office/data-protection-and-privacy/patlib.html

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 50

Name Off-site storage of PGP paper files

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG1 - 1 - Patent Granting Process

Entity Name - Processor (Entities)

External processors

POT and Zoons B.V. Databankweg 18 Amersfoort The Netherlands

External processors	
Name POT and Zoons B.V. Databankweg 18 Amersfoort The Netherlands, POT and Zoons B.V. Databankweg 18 Amersfoort The Netherlands	

Description of the processing

Description Paper originals submitted by users of the patent grant process of the EPO scanned on-site and kept on-site for a number of months in case scanning problems are detected. The original paper is stored in boxes.
After the initial on-site storage period the boxes are transported either from The Hague or Munich to the off site storage contractor POT to Amersfoort.
Here the boxes are stored in a secure warehouse. Upon request of the EPO (rare occurrence about 10 times per year) a document is requested to be retrieved from a box and to be sent back to the EPO either as original paper or as a scanned electronic version.
In line with the retention times, the EPO initiates safe destruction of the boxes. They are retrieved from the storage warehouse and transported to a specialized destruction company which carried out secure destruction.

Purpose of Processing Legal requirement Rule 147 EPC and PCT section 705bis

Data Retention Legal requirement is to keep the original paper submissions 5 years from the end of the year they were filed in.
Leaving one year safety margin the EPO has destroyed the scanned original paper older than 6 years.

Data subjects and categories of personal data

Employees

Contact Information	
Phone Numbers	
Employment Information	
Business Unit Division	
Personal Identification	
First Name	Full Name
Surname	

Externals

Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers

Recipient of the personal data

Recipients of the data At contractor: staff of POT
At EPO: staff of directorate 132 interacts with the contractor

Purpose of sharing Legal requirement Rule 147 EPC and PCT section 705bis

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) POT and Zoons B.V. Databankweg 18 Amersfoort The Netherlands - Netherlands

Transfer to public authority and/or International Organisation

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Transfer mechanism(s) The recipient provided appropriate safeguards

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures no privacy and security and risk assessment carried out by the EPO

Data protection statement

Data Protection Statement link internet
https://www.epo.org/about-us/office/data-protection-and-privacy.html

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 55

Name Pan-European Seal Farewell-Commencement Ceremony

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 02 - Communication

Entity Name - Processor (Entities)

External processors

External employees working at EPO in the Principal Directorate Communication.

External processors	
Name External employees working at EPO in the Principal Directorate Communication.	

Description of the processing

Description Principal Directorate Communication is, together with PES Team in Talent Acquisition, in charge of the organisation of the Pan-European Seal Farewell-Commencement Ceremony that will happen on September 17, 2021.

Meeting invitation email and reminders to the speakers and participants will be sent by PES team.

The digital event will take place via an online platform (MS Teams or Zoom) which all participants will be able to join by clicking on the link sent in the meeting invitation email.

In order to be able to promote the PES Programme in the EPO's internal and external channels at a later stage, vMix recording platform will be included in the main ceremony's platform. Additionally, pictures may be taken by audio-visual team.

The external provider Regiepapst will support Principal Directorate Communication and HR Talent Acquisition and Talent Academy in the organisation and recording of the event. They will also collect anonymised data for statistical purposes.

PES team may also made use of the Slido platform, which will be controlled by PD02, depending on the activity or presentation they have prepared.

Once the ceremony has ended, Regiepapst will send the video and statistical data to PD02. Audio-visual content will be used according to the purpose it was collected and for the period of time indicated below.

Data Retention PD Communication will store and process their data until 1 year after the end of their traineeship in order to promote the PAN-EUROPEAN SEAL.

Nevertheless, edited audio-visual material may be stored for further period according to the data protection statement for the processing of personal data in the context of recording and photographing by the Principal Directorate Communication that can be provided to the data subject upon request. According to it, the time limit for storage of the audio-visual material differs according to the following multimedia material classification:
• Historic: 25 years renewable
• Medium: 10 years renewable
• Low: 2 years renewable

Purpose of Processing - Create audio-visual content to promote the Pan European Seal (PES) programme through the different EPO internal and external channels, - Allow participants to join the Pan-European Seal Farewell-Commencement Ceremony

Data subjects and categories of personal data

Externals

Sensory and Electronic Information	
Audio Information	Electronic Information

Visual Information	
Contact Information	
Contact Details	
Personal Identification	
Full Name	Gender
Surname	Nationality

Employees

Contact Information	
Contact Details	

Recipient of the personal data

Recipients of the data • DG 4.2.1 - HR Talent Acquisition and Talent Academy: EPO colleagues in charge of the carrying on of the Pan-European Seal program.
• DG0 – PD02 – Communication: EPO colleagues in charge of managing and promoting the Pan-European Seal section.
• General public accessing EPO websites, or any other communication channel used by Principal Directorate Communication, such as news outlets or social networks (EPO has account on Facebook, Twitter, LinkedIn, YouTube and Instagram)

Purpose of sharing • DG 4.2.1 - HR Talent Acquisition and Talent Academy: EPO colleagues in charge of the carrying on of the Pan-European Seal program.
• DG0 – PD02 – Communication: EPO colleagues in charge of managing and promoting the Pan-European Seal section.
• General public accessing EPO websites, or any other communication channel used by Principal Directorate Communication, such as news outlets or social networks (EPO has account on Facebook, Twitter, LinkedIn, YouTube and Instagram)

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Explicit consent of the data subject

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer promote the Pan European Seal (PES) programme

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet To be added

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 56

Name Recording and photographing Isar Building under the “Isar daylight project”

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 02 - Communication

Entity Name - Processor (Entities)

External processors

Huddle

External processors	
Name Huddle	

External employees working at EPO in the Principal Directorate Communication.

External processors	
Name External employees working at EPO in the Principal Directorate Communication.	

Description of the processing

Description Under the Isar Daylight project, Principal Directorate Communication (PD02) is going to record and photograph (videos, pictures, interviews) and document the actions taken for publications to all staff, in the EPO’s annual activity report video and other internal or external information purpose. These recordings will be published mostly on the Office’s intranet or used as illustration in internal mails or for the info points (screens inside the office). Some recordings might also be used for external communication purposes (presentation to the Administrative Council and the 50th anniversary of the EPC) or if

relevant published on the Office's internet pages and other social media managed by the Office.

In some locations, it is also foreseen that a time laps camera is installed so that evolution over time can be monitored. During these recording it is likely that employees (internal and external) will be visible, they could hence appear in the final media product. In order to protect and comply with the right of every data subject to not appear in the final material, PD02 will take the necessary steps to ensure this by clearly indicating the days in which the recording will be made and blurring the faces or not including the recording when the person appearing is an external employee who has not provided his or her consent or an employee who has not volunteered (see below)

In addition, a call for interest is made so that PD02 records staff's feed-back and photographs them packaging/unpackaging their stuffs from the beginning of the work to the final result. Therefore, only EPO employees who volunteer and duly informed employees of the external suppliers who freely provided consent for such recording will be subject to this specific activity and the activity described above (time laps camera).

To complete this activity and in order to offer EPO employees different possibilities of participation, PD02 may also propose a voluntary activity that is to be published as a call for volunteers on Intranet in which people are invited to send to audio-visual team photos, personal images and recordings giving their opinion about the activity. PD02 will take in this case all the necessary measures as well as instructions to respect and protect the interested parties who appear in the photos.

External suppliers working on the project are contacted to be informed and asked for their employees' written consent. PD02 will take the necessary diligence to demonstrate that each of the employees concerned has consented to processing of his or her personal data. Each employee shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

The raw recording material will be edited so as to create short video's or "photo montage" which can be used for publication, these will then also be archived in the media database. The raw material will be discarded after editing, ultimately 1 year after the recording date.

Data subjects are informed about the recording or photographing by different mediums before and during the activity (data protection statement, news item on Intranet; email, signposting at the entrance and rooms where the recordings are taking place).

Purpose of Processing Documentation of the Isar Daylight project and use of the material to the promotion of the communication activities carried out at the EPO.

Data Retention The raw material will be discarded after editing, ultimately 1 year after the recording date.

The edited material will be stored according to the data protection statement for the processing of personal data in the context of recording and photographing by the Principal Directorate Communication that can be provided to the data subject upon request. According to it, the time limit for storage of the audio-visual material differs according to the following multimedia material classification:
• Historic: 25 years renewable
• Medium: 10 years renewable
• Low: 2 years renewable

Data subjects and categories of personal data

Employees

Sensory and Electronic Information	
Audio Information	Electronic Information
Visual Information	
Personal Identification	
First Name	Full Name
Surname	

Externals

Sensory and Electronic Information	
Audio Information	Electronic Information
Visual Information	
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data Multimedia material could be made available to:
• In a need-to-know basis:
 EPO external employees working in the Principal Directorate Communication
 The project manager and other EPO employees (internal and external) working on the Isar Daylight project, such as D444 Planning & Construction, and D4421 Facility Management MUN

• General public accessing EPO websites, or any other communication channel used by Principal Directorate Communication, such as news outlets or social networks (EPO has account on Facebook, Twitter, LinkedIn, YouTube and Instagram)

Purpose of sharing Social Media / PR

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Explicit consent of the data subject

Country where data might be transferred - Processor (Vendors) Huddle - United Kingdom

Reasons for the transfer Create audio-visual PR content

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet to be done

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 57

Name Tender procedures and agreements between external supplier and the EPO

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 011 - Chief Business Analyst

Entity Name - Processor (Entities) DG4 - 41 - Finance

External processors

Bidders / contractors

External processors	
Name Bidders / contractors	

Description of the processing

Description For most procurement procedures PD011 makes largely use of the administrative support of Central Procurement (CP), by participating to main phases and by approving the key proposed decisions (choice of procedure, choice of supplier, under art. 22a FinRegs and implementing rules), therefore the same description should apply as the one provided by CP to the DPO. The processing of personal data is necessary e.g. for:
- Registering the person/company applying for the tender (CP)
- for distribution and dissemination to the Award Committee (CP),
- to communicate with the person/company in the different phases of the tender processing (CP).
- To eventually invite the person/company to a meeting with the Award Committee to present their offer and answer questions.(CP)

Purpose of Processing Personal data is processed for the purpose of selecting a company to deliver product or services to the EPO following defined criteria and conditions and for accountability purposes

Data Retention Personal data will be kept by the EPO to following the legal obligations (directive on contract: Agreement No. 2016/3286 relating to the provision of consultancy services for surveys among patent applicants and first amending agreement No. 2017/3041) for keeping such category of data:
- the data is stored in FIPS and in physical original paper form in a closed room for accountability purposes for a maximum period of 12 years after the contract has been finalised behind lock in storage cabinets.
- contact details can be kept as part of a contact details database shared internally among EPO departments in order for them to contact data subjects for future tenders.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Working email address
Financial	
Bank Account Information	Bank Account Number
Personal Identification	
First Name	Full Name
Nationality	Signature

Employees

Contact Information	
Contact Details	

Recipient of the personal data

Recipients of the data Personal data depending on its type and the purposes of its processing is made accessible only on a need to know basis to EPO staff.

Different business units at the EPO will have access to the information stored on the contact details database on a need to know basis, e.g. in order for them to contact data subjects for future tenders.

Purpose of sharing Personal data depending on its type and the purposes of its processing is made accessible only on a need to know basis to EPO staff.

Different business units at the EPO will have access to the information stored on the contact details database on a need to know basis.

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation No

Transfer mechanism(s) A derogation in accordance with Art. 10 DPR

Reasons for the transfer Contact data of the EPO employee responsible for administrative matters is communicated to the bidders / contractors.

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 64

Name List of contact names to support settlement and safekeeping of securities

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 05 - Administration of Reserve Funds

Entity Name - Processor (Entities)

Description of the processing

Description The Administration of the Reserve Funds has appointed a custodian bank for the settlement and safekeeping of securities owned by the European Patent Organisation. BNP Paribas Securities Services was selected, and, for operational purposes, the personal data of its employees are stored in a EPO Database.

Data Retention he data is stored for the duration of the contract with the service provider.

Purpose of Processing Personal data of BNP Paribas Group employees are processed for the purpose of the settlement and safekeeping of securities.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Phone Numbers
Working email address	
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Personal Identification	

First Name	Surname

Recipient of the personal data

Recipients of the data Personal data are accessed for operational purposes by 0.5 staff. In exceptional cases personal data which part of contracts might be shared with the EPO legal department for legal due diligence purposes.

Purpose of sharing

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures All personal data related to the custodian bank employees are stored in secure IT applications according to the security standards of EPO. These include: • User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; • Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; • Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices; • Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; • Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; • Security incidence response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 65

Name List of contact names to support dealing in financial securities and cash management

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 05 - Administration of Reserve Funds

Entity Name - Processor (Entities)

Description of the processing

Description The Administration of the Reserve Funds makes use of various outside contractors (counterparties) for dealing in financial securities and cash management.
For operational purposes, contact details of these contractors is stored in an EPO Database.

Data Retention The contact details of outside contractors are stored for operational purposes as long as the contractor is still used for dealing in.

Purpose of Processing Personal data is processed for the purpose of dealing in securities.

Data subjects and categories of personal data

Employees

Sensory and Electronic Information	
Audio Information	
Contact Information	
Contact Details	

Externals

Sensory and Electronic Information	
Audio Information	

Contact Information	
Contact Details	Personal Email
Phone Numbers	Working email address
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data Personal data is accessed for operational purposes by 0.5 staff. In exceptional cases, personal data which is part of contracts might be shared with the EPO legal department for legal due diligence purposes.

Purpose of sharing

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures All personal data related to contractors is stored in secure IT applications according to the security standards of EPO. These include: • User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; • Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; • Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices; • Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; • Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; • Security incidence response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 66

Name List of contact names to support use of RFPSS investment management platform.

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 05 - Administration of Reserve Funds

Entity Name - Processor (Entities)

Description of the processing

Description The Administration of the Reserve Funds has appointed the external contractor SS&C London for a managed service of the RFPSS management platform (a set of services, tools and software for asset management). For operational purposes, the personal data of SS&C London's employees are stored in RFPSS files.

Data Retention The data is stored for the duration of the contract with the service provider.

Purpose of Processing The personal data of SS&C London's employees are processed for operational purposes.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Phone Numbers
Working email address	
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Personal Identification	

First Name	Surname

Recipient of the personal data

Recipients of the data Personal data is accessed for operational purposes by 0.5 staff. In exceptional cases, personal data which is part of contracts might be shared with the EPO legal department for legal due diligence purposes.

Purpose of sharing Operational and/or legal due diligence purposes.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures All personal data related to SS&C employees are stored in secure IT applications according to the security standards of EPO. These include: • User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; • Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; • Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices; • Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; • Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; • Security incidence response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 68

Name Customer Services Management (CSM)

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG1 - 1 - Patent Granting Process

Entity Name - Processor (Entities)

External processors

ServiceNow

External processors	
Name ServiceNow	

Description of the processing

Description Following the need to provide an improved customer service to handle incoming enquiries in an efficient, consistent and time-bound manner, the EPO concluded an agreement with a provider of modern Customer Services Management in order to replace current CRM (iExtensions). The software is a cloud-based application allowing to receive, process and monitor incoming customer enquiries (received by phone, mail or contact form) in a state-of-the art way permitting much better integration with MS Teams (while CRM still built on Lotus Notes). The user experience, reporting options and the ease of handling and monitoring will likewise be optimised with the new software.

At the EPO, when an enquiry is sent to support@epo.org or received either via the webform by contact@epo.org or by phone is received at the EPO, the sender data are compared against the contact details in our database to identify the sender and to allow a routing of their enquiry under these contact

details. This allows to automatically acknowledge receipt of the enquiry, update and reply to this user and to monitor any pending requests – in the interest to provide the best possible user experience.

The scope and purpose of the processing of personal data by the Data Processor on behalf of the EPO:

- Central Customer Database – Record personal information about external users / customers
- Case Management - Manage interactions and activities with external users /customers
- Activity Management - Store visit reports and/or information in respect of training event attendance of external users / customers
- Monitoring Timeliness SLAs / KPIs in respect of external users' / customers' enquiry resolution

The contact details are only needed, processed and stored in so far as they are required to handle user enquiries about EPO tools, pending applications for a European patent, International PCT applications, opposition and limitation/revocation files, patent information issues, products and questions, payment-related queries -about questions, actions and issues which are linked to the mission and services provided by the EPO.

The enquiries and the replies thereto are in no way intended to replace and/or bypass the existing rules and ways of communication. The procedures before the EPO remain within the remits of the EPC and the PCT and our CSM will not go beyond or deviate from this. Also is it not foreseen to record any calls. The questions received and answers given are meant to support and supplement the written procedure and find exactly their limit where the written procedure takes precedence.

This processing does not apply to procedural activities and steps as foreseen under the EPC are not allowed to be performed this way (these have to be traditionally done in writing using one of the communication means as decided by the President).

Anonymized data are also used for statistical purposes and trends watching. Nevertheless, individual users are not identifiable. Statistical data is used to gather information only about the categories of users or the types of issues they address.

Purpose of Processing To handle incoming enquiries, to receive and to reply to a question/query/issue addressed to the EPO, ranging from questions on our filing services to procedural patent application-related queries.

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which it is processed. Personal data will be stored as long as the processing is operational.
Content of the tickets will be segregated from the contact details.
Contact details will be stored for five years after they have been used or updated the last time, i.e., after the last interaction with their subject within the framework of Customer Services Management.
Personal data received with an enquiry will be anonymized 5 years after the closure of a particular ticket, allowing the anonymised data to be used for statistical purposes.

In the event of a formal appeal/litigation, all data held at the time of the formal appeal/litigation shall be retained until the completion of its process.

In any case, data are deleted at the request of the user concerned.

Data subjects and categories of personal data

Externals

Ticketing	
Ticket related data	
Contact Information	
Contact Details	Personal Email
Phone Numbers	Working email address
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Personal Identification	
First Name	Surname

Employees

Ticketing	
Ticket related data	
Contact Information	
Contact Details	Personal Email
Phone Numbers	

Personal Identification	
First Name	Surname
User Account Information	
User ID	

Contractors

Ticketing	
Ticket related data	
Contact Information	
Phone Numbers	Working email address
Employment Information	
Office Location	
Personal Identification	
Full Name	
User Account Information	
User ID	

Recipient of the personal data

Recipients of the data - BIT Administrators and Application Domain Managers, DG4, Corporate Services
- DG1 PD-USQM, D13, User Services and Quality Management
- DG1 Operations, DG1, Directorates and OCFDs
- DG4 Finance, D412, Revenue Controls
- DG5 Patent Knowledge and Publication, D54, Patent Knowledge
- DG5 Patent Law and PCT International Legal Affairs, D52, Patent Law and PCT Int. Legal Affairs
- DG0 - PD Communication, D022, Channel Management

There is no segregation of data as information sharing is necessary for reasons of maintaining efficiency. However, complaints, due to their sensitivity, will only be handled by a designated agent (limitations in the access rights).

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures All personal data processed in the systems hosted at the EPO premises are stored in secure IT applications according to the security standards of EPO. These include: - User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. - Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. - Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices. - Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices. - Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk. Security incidence response: 24/7 monitoring for incidents, on-call security expert' For personal data processed on Service Now systems, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: - Physical security measures. - Access control measures: role-based, principles of need-to-know and least privilege. - Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. - User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, antimalware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management. - Transmission control measures: audit logging, System and network monitoring. - Input control measures: audit logging, System monitoring. According to an internal security review and following the information from the ServiceNow Trust and Compliance Center, their operations cover all areas of ISO27001 and are in line with the EPO 'Cloud Computing Guidance Note v1.1'. According to this evaluation (which has been provided as evidence and proof for the contract with ServiceNow), the criteria of … - Service Availability/Disaster Recovery Confidentiality - Security and Integrity - Auditability - Cloud and Provider Location - Reversibility/Portability/Exit - Provider's Reliability and Solvency/Insurance - Certifications … have been successfully met. Provider's security framework is based on ISO/IEC 27002:2013. It has been an ISO 27001 certified organization since 2012 and is also ISO/IEC 27017:2015 and 27018:2019 certified. Provider

also applies industry recognized information security frameworks. These include ISO/IEC 27001:2013, ISO/IEC 27017:2015, and 27018:2014, as well as accreditation with regional standards and regulations., For transfer of personal data, the provider uses a controlled access feature hopping (HOP) functionality. This is an extension of the production cloud environment and allows authorized employees (“users”) to access and handle customer data, with the prior consent of the customer, in a controlled environment which maintains controls to restrict data from being exfiltrated. These functionalities reduce the probability that customer data and assets will be compromised. The provider also has appropriate internal regulations and policies that define exactly how data should be handled.

Data protection statement

Data Protection Statement link internet
Under preparation

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 75

Name European Patent Register

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities) DG1 - 1 - Patent Granting Process, DG5 - 54 - Patent Knowledge

External processors

Microsoft

External processors	
Name Microsoft, Microsoft	

ServiceNow

External processors	
Name ServiceNow	

Description of the processing

Description According to Article 20 EPC, the Legal Division (embedded in PD 5.2 legal affairs) shall be responsible for decisions in respect of entries in the Register of European Patents and it therefore administers the European Patent Register.
The Legal Division performs its duties in accordance with the Decision of the President of the European Patent Office dated 21 November 2013 concerning the responsibilities of the Legal Division.

The personal data necessary to perform the related processing operations (i.e. the information

concerning documents pursuant to Rules 14 EPC, 22 EPC, 23 EPC, 24 EPC, 142 EPC or R142 EPC) is received mostly internally from a DG1 formalities officer via a Madras mailbox message in the legal division (in exceptional cases, the personal data can be received by fax or post), when guidance/legal advice is needed (Rule 22 EPC) or the procedural step (Rule 142 EPC) belongs to the responsibility of the legal division.

A member of the legal division makes an assessment and takes a decision on whether an update or a change on the register is necessary. In isolated cases the matter might necessitate legal advice (see corresponding record on legal advice). The registration of the decision is done in Madras.

The European Patent Register is being updated automatically following the registration. A communication informing the relevant party is usually sent by post by the legal division or, in case the representative has a dedicated Madras mailbox, the communication is notified automatically to him there. In some specific cases, the notification takes place via DG1 formalities officers (depending on the EPC Rule).

In case a request reaches the legal division via DG1 ticketing system: The ticketing system sends automatic emails to the mailbox of the legal division, those emails do however not entail any personal data, they only provide a ticket number and a link to access the ticketing system. The requester receives the answer via this ticketing system. In exceptional cases, when the requesters have further questions, they can contact directly the legal division via email. in such case corresponding personal data is shared via email.

All documents filed in the proceedings are stored in Madras.

The data subjects concerned are applicants, representatives, opponents, third parties and inventors pursuant to Rule 21 EPC.

Further personal data may be processed if sent by the parties, especially the information triggering the potential change of the register (e.g according to the Rule 22 EPC, the documents providing evidence of a transfers of an a European patent application). In some cases, such personal data is of sensitive nature (e.g., medical reports). Possibly personal data related to health in cases regarding Rule 142(1)(a) EPC.

Data Retention For reasons of legal certainty, personal data is kept for an indefinite period.

Purpose of Processing The described processing activities are required for the legal division to administer the European Patent Register.

Data subjects and categories of personal data

Externals

Ticketing	
Ticket related data	

Health Data	
Health Data	
Contact Information	
Contact Details	Phone Numbers
Working email address	
European Patent Register Data	
Address	Data provided by the data subjects
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Personal data potentially included within the content of a patent (claims, description, drawings, abstract)	
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
Employment Information	
Business Unit Division	Company Entity
Department name and/or number	Job Title Role
Language preference (of communication)	Office Location
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	
Government Identifiers	
National Identity Card Details	Passport Number

Employees

Employees

Contact Information	
Contact Details	Phone Numbers
Employment Information	
Business Unit Division	Job Title Role
Office Location	Personnel Number
Personal Identification	
Full Name	Signature

Recipient of the personal data

Recipients of the data 1) EPO internal Madras users
2) The public
3) trustees outside Member States.

Purpose of sharing 1) EPO internal Madras users have access to all data filed thereof.

2) The public has access to the data that is visible in the European Patent Register.

3) In some Rule 142 EPC cases, trustees outside Member States are notified of the information published in the European Patent Register.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, ServiceNow - Australia, ServiceNow - United States, ServiceNow - India, ServiceNow - Japan, ServiceNow - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Informing Trustees is part of the European Patent Register tasks

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case, The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 76

Name SACEPO meetings

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 46 - CIO / BIT

External processors

SAP

External processors	
Name SAP	

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft	

OpenText

External processors

Name
OpenText

Members of Sacepo

External processors
Name
Members of Sacepo

Description of the processing

Description A dedicated advisory body, the Standing Advisory Committee before the European Patent Office (SACEPO), was created in 1978 at the same time as the Office opened its doors, in order to involve users in the development of the European patent system. SACEPO brings together a wide range of experienced patent attorneys and representatives of industry (including small and medium-sized enterprises) to conduct a general review of EPO activities of the past year and projects for the future. Regular meetings hosted by the EPO President are held once a year. In addition, meetings of five specialist SACEPO Working Parties (Quality, Rules, Guidelines, Patent Information and E-Patent Process), dedicated to more technical matters, take place on a regular basis during the year.

The relevant personal data of SACEPO members, already collected during the SACEPO membership selection process, are used by the delegated controller to organise the above mentioned meetings.

All email exchanges as from the preparatory phase of the meetings until the following up exchanges after those, including sharing of minutes, are conducted through the SACEPO mailbox (SACEPO@epo.org) of the delegated controller.

The meetings are chaired/run by the President of the EPO or another EPO representative. Corresponding preparatory phase requires the sharing of information through the Common Log (internal EPO tool). Further EPO staff or, exceptionally, external experts are present as and when needed. MS Teams collaborative platforms can be set up to facilitate engagement between the participants to those meetings (SACEPO members and experts, and EPO senior experts/team managers).

While meetings occur virtually since the covid pandemic, physical meetings remain possible. Should the travel and/or accommodation costs of SACEPO’s members be borne by the EPO, corresponding form would have to be filled and accompanied by justification documents. Should the Office organise a lunch or dinner, the participants might be asked about dietary needs.

After the meetings, the anonymous minutes are distributed to attendees via email. Other additional information related to the content of the presentations/discussions is usually distributed also.

Purpose of Processing The processing is necessary to plan, organise and run the consultation of the users of the patent system by this dedicated advisory body, the Standing Advisory Committee before the European Patent Office (SACEPO), created in 1978 This encompasses: 1. Organisation and holding of the meetings 2. Distribution of documents, agendas and minutes related thereto 3. In case of physical meeting, data necessary for e.g. reimbursement of travel and accommodation, dietary requirements 4. In case of virtual meetings, technical support as might be necessary 5. Preparation of the meetings by the EPO’s officials involved. 6. Keep track of the consultation process for future reference and archiving.

Data Retention Should dietary requirements have been collected, this data is deleted after the event and latest after 3 months

Should invoices be sent to the delegated controller, (the case be) Invoices are kept for three years.

Other personal data of members of SACEPO processed in relation to those users' consultations is kept for three years after the elapsing of their SACEPO membership.

The anonymous Minutes of SACEPO meetings are kept without limitation of time.

Data subjects and categories of personal data

Externals

General	
User association	
Health Data	
Dietary requirements	
Contact Information	
Contact Details	Home Address
Phone Numbers	Working email address
Professional Experience & Affiliations	
CV	Professional Memberships
Qualifications Certifications	
Correspondence	
Personal information provided voluntarily	
Financial	
Bank Account Information	
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Personal Identification	
First Name	Surname
Nationality	

Employees

Health Data	
Dietary requirements	
Contact Information	
Contact Details	Working email address
Employment Information	
Business Unit Division	Job Title Role
Personal Identification	
First Name	Gender
Surname	

Recipient of the personal data

Recipients of the data - Internal participants to the meetings
- External participants, business associations whose delegates are SACEPO members
- Presenters and EPO senior management
- Technical Services
- Financial services
- External providers

Purpose of sharing - Sharing with participants is necessary to achieve the main purpose of the meetings (e.g. list of participants, minutes, documents)
- Upon request of interested parties, such as business associations whose delegates are SACEPO members, the EPO might decide to share the SACEPO meetings' material (agenda, documents, minutes) with those.
- EPO Presenters and EPO senior management share a meeting file including background on participants
- Technical Services (if necessary; only relevant contact data is shared)
- Financial services (as necessary for reimbursements)
- External contractors for service providing.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OpenText - United States, SAP - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 77

Name Disciplinary procedures against professional representatives before the EPO

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - Chairman of the Disciplinary Board of the EPO

Entity Name - Processor (Entities) DG4 - 44 - General Administration

External processors

zoom

External processors	
Name zoom	

Microsoft

External processors	
Name Microsoft	

Data subject or his representative if located outside EEA

External processors	
Name Data subject or his representative if located outside EEA	

Description of the processing

Description Infringements of the Rules of Professional Conduct of Professional Representatives may be considered by the

following bodies (See Article 5 Regulation on discipline for professional representatives; hereafter “RegDisc” as well as Additional Rules of Procedure of the Disciplinary Board of the European Patent Office hereafter “AddRules”):
(a) the Disciplinary Committee of the Institute of Professional Representatives before the European Patent Office (hereinafter “DC of the EPI”)
(b) the Disciplinary Board of the European Patent Office (hereinafter DB of the EPO)
(c) the Disciplinary Board of Appeal of the European Patent Office (hereinafter DBoA)

(a) Involvement in procedure with the Disciplinary Committee of the EPI
The Chair and the registrar of the DB of the EPO are involved incidentally during proceedings with the DC of the EPI (item (a) above). The processing operation is triggered by the receipt of the notification by the Disciplinary body of the EPI, to allow the application of Article 6 RegDisc, per email. These provisions require the close involvement of the chairman and of the registrar of the DB of the EPO, monitoring time lines and taking decisions of procedural nature. A corresponding file is created by them in a confidential shared-drive. This involvement leads either to the closure of the case or to a further processing, should the matter be brought before the Disciplinary Board of the EPO:Procedure with the Disciplinary board of the EPO.

(b) Procedure with the Disciplinary board of the EPO

This procedure is triggered either by a decision of the DC of the EPI or by the chairman of the DB of the EPO (Article 6 RegDisc). The transmission of the relevant file from the DC of the EPI to the DB of the EPO as well as the information of the professional representative are regulated by Article 6 AddRules. The professional representative concerned can also be requested to provide directly further information/documents. This collection of personal data takes place via email or registered post. The registrar stores those in the dedicated mailbox (disciplinaryboard@epo.org) and computer, and stores the file in a dedicated shared-drive.

The operations necessary for the procedure with the DB of the EPO encompasses:
- Launching the procedure, information of DB members, conduct of preparatory inquiries, designation of rapporteur, organising the exchange of written submissions by the parties,
- the holding of oral proceedings in person or in virtual environment (video conferences), which necessitate the drafting of minutes and might involve the audio recording of the meeting (See e.g. Art 7 AddRules),
- the participation of further data subjects such as witnesses, legal practitioner, interpreters, President of the EPI, President of the EPO,
- All activities of the DB of the EPO, including deliberations, voting, decision making, necessitating regular meetings in person or in virtual environment (video conferences).
The video conferences may take place via Zoom

Purpose of Processing The personal data is processed to enable the Disciplinary Board of the EPO or, the case be, its chairperson or registrar, to perform the tasks with regard to the discipline against Professional Representatives (See Regulation on discipline for professional representatives (OJ EPO 1978, 91, OJ EPO 2008, 14); Additional Rules of Procedure of the Disciplinary Board of the European Patent Office OJ EPO 1980, 183 OJ EPO 2007, 552, 555) which encompass - Organising and monitoring administrative steps to allow o timely and informed Decisions, as foreseen in the applicable provisions o planning and organising the work of the DB of the EPO o report on these activities when required, including with the provision of anonymous statistics - keep track of past decisions in case the same individual is involved in or subject of further disciplinary procedures, or in case of related litigation. - Keep track of past procedures to allow an harmonised and consistent approach of the DB, also to ensure legal certainty.

or Teams.

This procedure ends with the final decision of the DB of the EPO to dismiss the matter or to impose penalties. The decision might have to be notified to the Legal division of the EPO (Art 28(2) RegDisc), or be published under certain conditions and in an anonymised way as provided in the applicable rules (Art 16 AddRules). The final decision means the end of the active processing of the file by the DB of the EPO.

(c) Procedure with the DBoA
The DB is not involved in this procedure.

The files of the DB of the EPO are kept until the end of the applicable retention period(s).

Data Retention In cases not leading to a disciplinary sanction, the retention time is 5 years from the date of the decision of the DB.

In case leading to a disciplinary sanction, the retention time is 10 years from the date of the decision of the DB.

However, should a related litigation have been launched and the above time line have elapsed, the file is kept for 5 years after the end of the litigation.

After the elapsing of the applicable retention time, only the complaint and the decision are kept.

The minutes are submitted to the parties prior to their adoption. Once the minutes adopted, the recording is deleted.

Data subjects and categories of personal data

Externals

Health Data	
Health Data	
Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers
Working email address	
Professional Experience & Affiliations	
CV	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
European Patent Register Data	

Address	Data provided by the data subjects
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Personal data potentially included within the content of a patent (claims, description, drawings, abstract)	
Employment Information	
Company Entity	Job Title Role
Language preference (of communication)	Office Location
Previous Work History	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Nationality
Picture	Signature

Employees

Contact Information	
Contact Details	Home Address
Phone Numbers	Working email address
Employment Information	
Room Number	
Personal Identification	
Digital signature	Full Name
Signature	

Recipient of the personal data

Recipients of the data Respondent(s) of the disciplinary case (professional representative against whom the breach of the Rules of professional Conduct is alleged), representative of respondent of the disciplinary case.
Chairman of the DC of the EPI (see e.g. Art 6 RegDisc), Presidents of the EPO and of the Council of the Institute of professional representatives (see e.g. Art 12, 14 and 21 RegDisc):
External disciplinary Board members (access to the whole file).

The president of EPI receives the decision according to Art 21 RegDisc) as well as communication giving him the opportunity to comment before final decision is taken Art 12 RegDisc
BoA receives the DB cases from DB of the EPO in case an appeal is filed to a DB decision
Complainant / or representative of complainant is informed of the result of the proceedings (Art21 RegDisc)
Respondent as well as their representatives receive the decision as well as communication giving him the opportunity to comment before final decision is taken Art 12 RegDisc
The case be, interpretors

Note: The internal disciplinary board members, the registrar of Disciplinary board and staff of D523 supporting the Chairperson in the exercise of this independent function are considered as belonging to the delegated controller's unit for the purpose of this record, and are thus neither considered as recipients or internal processors.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, zoom - Unknown

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Communication with data subjects or their representatives

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 79

Name Organisation of meetings with the US Bar-EPO liaison Committee

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft, Microsoft	

OpenText

External processors	
Name OpenText	

Description of the processing

Description The US Bar-EPO Liaison Council was created as a forum to facilitate exchange between the EPO and US applicants. It serves to increase mutual understanding of European and US patent practice, and update members on recent developments on both sides of the Atlantic.
The US Bar-EPO Liaison Council is an US Organisation with its own statutes, created by US Stakeholders in 1984. The annual meetings usually take place alternately at the EPO and in the US.

When the meeting takes place at the EPO, the personal data necessary to the organisation of the meetings, including professional background of participants, is requested by D522 from the US Bar-EPO Liaison Council Chair. Other participants are usually Office employees. The requested information is usually received via email.

The data, received by email and manually stored on the w: drive, is used by the EPO (Dir 522) to organise the meeting and communicate all related information. Standard EPO tools are used: Microsoft Office 365, CMS (Case Management System) of legal affairs (see dedicated record), OpenText.
This includes sharing information with relevant stakeholders:
- Technical aspects to be dealt with for the meeting itself (e.g. digital platform)
- Exchanges prior to the meeting, e.g. for the preparation of the agenda, presentations, and president meeting file. D.522 liaises with the President's Office for the date and the file and the Protocol unit, should there be meals organised at an in-person meeting.
- Exchanges after the meeting, including sharing presentation materials, and other EPO documents, possible follow-up actions etc
- In case of physical meeting with organisation of a dinner, additional personal data might be processed related to dietary requirements provided on a voluntary basis by the participants.
- The list of US delegates is sometimes used to identify US candidates for SACEPO.

Data Retention - Meeting files and emails are stored for 20 years. Particularly important files might be archived beyond this time period.

- The Excel tables containing contact data are destroyed after 10 years.

- Should dietary requirements have been collected, this data is deleted after the event and latest after 3 months

Purpose of Processing Allow informal exchanges between the EPO and US applicants with a view to increase mutual understanding of European and US patent practice and to update members on developments on both sides of the Atlantic. This encompasses: - Setting up of physical or virtual meetings - Keeping track of previous exchanges and of related context - Plan future events - Maintain a database of experts in US patent law for future consultation, including in order to select potential US participants in SACEPO.

Data subjects and categories of personal data

Employees

Matter/Log file

Attachments	Metadata
Health Data	
Dietary requirements	
Contact Information	
Contact Details	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	
Employment Information	
Business Unit Division	Job Title Role
Personal Identification	
First Name	Surname

Externals

Matter/Log file	
Attachments	Metadata
General	
Any other information	User association
Health Data	
Dietary requirements	
Contact Information	
Contact Details	
Professional Experience & Affiliations	
CV	Professional Memberships
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Employment Information	
Company Entity	Job Title Role
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data - Chair of the US Bar-EPO Liaison Council, internal (EPO) participants (usually from DG1 and DG5) and external participants of the US Bar Liaison Office.

- Senior managers of the Office, usually President of EPO, Vice-Presidents DG1 and DG5, Chief International and Legal Officer.

- Presenters (internal EPO employees, usually from DG1 and/or DG 5), selected for their expertise in the field(s) to be discussed at a meeting.

Purpose of sharing - Chair of the US Bar-EPO Liaison Council, internal (EPO) and external participants of the US Bar Liaison Office: list of participants and documents shared as a preparation or follow up of a meeting.

- Senior managers and EPO presenters have access to the meeting file (Common Log) drafted within the delegated controller's principal directorate and submitted to the President of the Office for the sake of the organisation and preparation of the meeting. This entails information on participants and their professional background.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OpenText - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 81

Name Legal advice on contractual, (pre-)litigation and other general matters by Directorate 5.2.4 – Contract law and litigation

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft	

External Law Firms

External processors	
Name External Law Firms	

Description of the processing

Description D524 receives requests from other EPO units requesting for legal advice in contractual, litigation and general matters. Such requests are received by D524 via e-mail (e. g. Outlook), orally or in writing. All requests are registered in the Case management System (CMs) of the Directorate under a specific Log number together with the requester’s and responsible officer’s names and assigned to a responsible lawyer within the Directorate.

Once the request has been assigned to the responsible lawyer the legal question is identified, assessed, and answered to the requester via e-mail, orally or in writing.

The CSM is subject of a separate record.

Purpose of Processing Personal data is processed for the purpose of the EPO's administrative functioning, here in particular providing legal advice on matters within the responsibility of D 5.2.4: • giving Legal advice on matters of contractual and general legal nature, such as private and public building / construction law and all aspects of IT law, as well as memoranda of understanding and service level agreements; • identify and manage the legal risks which the Office faces in its activities; • support colleagues in the operational units and in Central Procurement in procurement matters, in particular in the preparation, drafting, negotiation and implementation of contracts; • vetting of contracts and CA documents according to Art. 1 ff of the Directive on contracts • assisting the operational units with the appropriate management of contracts, helping monitor the legal aspects to prevent issues before they arise; • maintaining an up-to-date, fit-for-purpose database of model contracts in different areas; • providing training and information on legal matters to stakeholders across the Office; • providing legal advice and support relating to litigation issues (with the exception of employment disputes), including on the avoidance of litigation (mediation, settlement), and oversee and coordinate any litigation efforts; • legal administration and management of the portfolio of intangible assets of the Office, such as trademarks and copyrights. • supporting the realisation of the Strategic Plan 2023, and assisting in the associated programmes and projects. • assisting in the managing and distribution of files and coordinating follow-up activities, as well as for accountability purposes. This is necessary for giving legal advice. Relevant provisions are: Rule 3.2 Tender Guidelines, point 6.5.2 of the Directive supplementing certain provisions of the Tender Guidelines, Directive on contracts.

Data Retention Personal data processed are stored for the period of time necessary to achieve the purpose for which they have been processed. contract related files: D 5.2.4 is asked to advise on drafting of a contract (see “Definitions” section in the Directive on contracts) and issues a legal approval for a given contract, and this contract is also concluded between the EPO and the contractor. D 5.2.4 physically destroys the corresponding file 12 years after termination of this contract (e. g. contract concluded on day 0 for delivery of items six weeks later, items are delivered 8 weeks later, file is destroyed 12 years after performance; framework contract concluded on day 0 for duration of five years, terminated already after 3 years, file is destroyed 12 years after termination) all other cases: D 5.2.4 gives a general legal advice that is not covered by the description above. File is physically destroyed 30 years after completion of this file.	

Data subjects and categories of personal data

Employees

General	
Any other information	Assessment and legal opinions
Contact Information	
Personal Email	Phone Numbers
Working email address	
Correspondence	
Any other information	Personal information provided voluntarily
Employment Information	
Assessment and legal opinions	Business Unit Division
Personal Identification	
First Name	Surname

Externals

General	
Any other information	Legal opinions and assessments
Contact Information	
Home Address	Personal Email
Phone Numbers	
Correspondence	
Any other information	Personal information provided voluntarily
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data Personal data will only be shared on a strictly need to know basis.

In general, personal data may be included in various communications or legal documents sent within the EPO for information and consultation of operational units or involved employees for the purpose described above.

In case of consultation of a law firm, D524 might have to share personal data with them.

Purpose of sharing In general, personal data may be included in various communications or legal documents sent within the EPO for information and consultation of operational units or involved employees for the purpose described above.

In case of consultation of a law firm, D524 might have to share personal data with them.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, External law firms providing legal consultancy services

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 82

Name Maintenance of List of professional representatives

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft, Microsoft	

ServiceNow

External processors	
Name ServiceNow	

Description of the processing

Description A natural person (external) must be registered on the list of professional representatives to be entitled to act as a professional representative before the EPO.

The Legal Division is responsible for:
- decisions on registration on and deletion from the list of professional representatives in accordance with Articles 20 EPC, 134 EPC, Rule 154 EPC, the notice from the EPO of 12.05.2015 concerning representation before the EPO (OJ EPO 2015, A55) and the decision of the President of the European Patent Office dated 21 November 2013 concerning the responsibilities of the Legal

Division, OJ EPO 2013,600,
- entry in the European Patent Register, Rule 143(1)h EPC,
- entry in the EPO searchable database.

The request for entry on the list of professional representatives is related to the passing of the EQE exams, apart from special circumstances such as accession of a State to the EPC. Relevant personal data is collected from the data subjects via specific forms (EPO Form 52300 or 53203), to be sent to the legal division in paper form together with supporting documents. Alternatively, the request can be done online using an electronic platform.

The deletion from the list of professional representatives is either triggered by a request (preferably using EPO form 52306) or information from the Institute of Professional Representatives before the EPO (epi) (deletion ex officio), the disciplinary board, or others (e.g. dependants, employer). For the processing of deletion from the list of professional representatives, special documents (including personal data and, possible special categories of personal data) are required depending on the grounds of the deletion.

The maintenance and publication of an up-to-date information status is one of the main activities performed. Any change of name/address or other details in the list of professional representatives before the EPO must be sent to the EPO Legal Division, preferably using EPO Form 52301 and 53201a.

The legal division provides other Office's units or external stakeholder (epi) with relevant information necessary to perform tasks associated with being a professional representatives, e.g. to ensure the publication, preparation of EPO badges for professional representatives, to allow invitation to specific events, seminars, surveys etc. Other contact detail exports or statistics can be provided internally, on request.

Most personal data are provided by the professional representatives themselves. Other sources apply sometimes, such as lists of successful candidates by EQE or information provided by epi.

System description:
Documents are usually received by post or email. All paper documents are scanned, sent in pdf format via Outlook (generic email address of the legal division) and stored in folders by date. These PDF-documents are stored in the D523 Tele-Archive folders sorted by date, name, CDS ID number, filing number and country on the EPO Shared-Drive (w: drive). Entry requests and the deletion procedure ex officio are monitored via Excel files on the EPO Shared-Drive (w: drive). Those files are only accessible by the legal division.
The legal division enters the relevant data in the database CDS (Client Data System, part of Madras, owned by Directorate-General 1), used mostly by formality officers.

Purpose of Processing The processing of personal data is necessary for the setting up, maintenance and publication of the list of professional representatives by the Office and providing up-to-date information to stakeholders as well as all associated actions to e.g. ensure a proper and efficient information flow and management of associated activities. This encompasses: – Entry on, and deletion from, the list of professional representatives and in the European Patent Register – publication in the EPO Official Journal, Announcement of the list of professional representatives before the EPO, publication on the searchable database – ensuring that the Institute of Professional Representatives before the EPO is provided with the personal data necessary to administer the data subjects' Institute membership, intrinsically related to being entered on the list of professional representatives – provide Office's units with information necessary to perform tasks associated with being listed as professional representatives - Preparation of statistics

CDS generates an ID-Code for each new entry of a professional representative. Furthermore, CDS records history data of actions and links the professional representative role to relationships like membership of a registered association or appointment as an authorisee in a general authorisation. CDS is used by DG1 to combine several types of information about different roles, acting addresses, including the link to dedicated filings. The Legal Division is the sole data owner of the role of professional representative and the main address in CDS. Any change of data or status could have direct impact on the representation in patent procedures (DG1). A daily export of the data of professional representatives is retrieved from CDS to DG5Admin, which is an application built on the Microsoft stack, using .NET, IIS, SharePoint, and Excel with VBA, hosted by the EPO Data Centre in Luxembourg. The export includes the number of applications linked to the professional representative, which is used for analytical statistics, like the number of most active representatives. DG5Admin processes data, statistics, exports, data consent registration and is generating Share point templates and Word documents. In addition, an Excel statistic template is used to generate anonymous figures about the actions performed in CDS, trigged by action date and type of change.

Data Retention For reasons of legal certainty, personal data is kept up to 99 years, starting from the first entry date on the list of professional representatives.

Data subjects and categories of personal data

Externals

Ticketing	
Ticket related data	
Health Data	
Health Data	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
European Patent Register Data	
Address	Data provided by the data subjects
Correspondence	

Personal information provided voluntarily	
Representation in EPO’s Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Role in the Patent Grant Procedure
Supporting documentation	
Browsing Information	
IP Address	
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Previous Work History	
Personal Identification	
Age	Date of Birth
First Name	Full Name
Gender	Surname
Nationality	Signature
Government Identifiers	
National Identity Card Details	Passport Number

Employees

Ticketing	
Ticket related data	
Contact Information	
Phone Numbers	Working email address
Employment Information	
Business Unit Division	Job Title Role
Office Location	Personnel Number

Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data Apart from the publicly available data published in the OJ and/or in the searchable database of the EPO:

Different business units at the EPO will have access to the information stored on the list of professional representatives on a need to know basis:

• DG5 Editorial Office: EPO Official Journal (name, former name if applicable, nationality, address, deletion reason indication like death)
• DG5 Publication European Patent Bulletin (EPB): Public notification of decision if its delivery has proven to be impossible
• DG4 Online Solutions Team: Online database of professional representatives (according to consent form public data)
• DG4 Access card management system: Nexus Prime application for issuing the EPO badges (following data is export from DG5 to DG4: name, surname, email address, CDS ID code, entry and deletion date from the list of professional representatives)
• DG1 Central Enquiries Unit (Support): CSM-Ticket database (CSM: Customer Services Management system)
• DG1 has access to CDS and CDR (PA DG1) receives copy of change requests (PDF-Files) in Shared drive folder
• Other internal contact detail exports or statistics on request for DG0, DG1, DG5
• Other involvements: Board of Appeals in case of an appeal (paper copy)

Institute of professional representatives, regular data transmission regarding the status of the professional representative and the membership payment of epi subscriptions.

Purpose of sharing Fulfil the purpose of the existence of the list of professional representatives.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Microsoft - United States, ServiceNow - Australia, ServiceNow - United States, ServiceNow - India, ServiceNow - Japan, ServiceNow - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 83

Name Activities related to pre-litigation and litigation on civil service matters where the Administrative Council is competent appointing authority

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities) DG4 - 44 - General Administration

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft, Microsoft	

OpenText

External processors	
Name OpenText	

Description of the processing

Description Administrative and judicial means of redress are available to EPO staff.

Where a dispute involves the Administrative Council as appointing authority, Legal Affairs assists by providing case management and legal services at pre-litigation (management review and appeal) level. This includes :
- collecting relevant facts and evidence, analysing and advising on the case
- preparing documents to be submitted to the Council
- preparing submissions to be submitted on its behalf by PD 52 acting as representative in internal appeal proceedings
- assisting in alternative dispute resolution attempts.
if a case reaches litigation level, the Organisation is represented by another unit in the judicial proceedings before the ILOAT. Legal Affairs will at this stage provide assistance to the representative and prepare any documents to be submitted to the Council in relation to the case.

For this activity, personal data of the persons directly or indirectly involved in a dispute (mostly staff members, former staff members or their dependents as claimants but also legal representatives, witnesses, case handler etc.) are processed, partly by automated means.

Information related to a case, including personal data, are collected via pleadings and evidence submitted from the parties to proceedings, third parties (e.g. witnesses), publicly available sources (e.g. internet searches), or gathered from other Office's units in the course of fact-finding activities when preparing a case (e.g. HR, manager). The personal data collected from the parties' submissions can be about them or others. The personal data so collected may occasionally include special categories of data. The categories of personal data processed depends on the subject matter of a case.

Information related to a case is stored electronically in a document management system and in the files kept by Legal Affairs. In some cases, a paper file is created.

Information related to a case are used in documents produced along the proceedings and exchanged between the parties or submitted to consultative (Appeals Committee) and decision-making (Administrative Council).

Information related to a case is shared within the Office as necessary for example to allow verification of factual elements, to inform or consult other services, to request translation, or in the course of approval process.

Information related to a case is transmitted outside the Office as necessary, for example when an external attorney is involved or other experts are consulted (e.g. tax expert).

References to cases are included in lists kept for monitoring pending litigation, for reporting and for statistical purposes.

Purpose of Processing Personal data is processed for the purpose of the EPO's administrative functioning, here in particular: 1- for assisting and/or representing the Administrative Council throughout administrative or judicial proceedings initiated against its decisions. 2- enabling the availability of dispute files for later reference in the event of subsequent litigation 3 – for archiving and statistical purposes.

Data Retention Personal data processed are stored for the period of time necessary to achieve the purpose for which they have been processed.
In the absence of a specific reason to retain a file:
Litigation that led to a judgment from the ILOAT:
* 10 years after the judgment was pronounced the parts of the file relating to the precedent stages of litigation, are destroyed.

* 15 years after the pronouncement of the judgment, all parts are destroyed.

Litigation that did not lead to a judgment from the ILOAT:
* 10 years after the closing of the last internal stage of proceedings, all parts of the file other than the advisory opinion and the decision closing the stage of proceedings are destroyed.

* 15 years after the closing of the last internal stage of proceedings, all parts are destroyed.

This applies to both electronic and paper files.

An index of cases with limited personal data categories (reference, name, status) is kept indefinitely.

Data subjects and categories of personal data

Employees

General	
Assessment and legal opinions	
Health Data	
Health Data	
Contact Information	
Contact Details	
Professional Experience & Affiliations	
Trade Union Membership	
Correspondence	
Personal information provided voluntarily	
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name

Employment Information	
Appeals Records Information	Assessment and legal opinions
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Disciplinary Action
End Date and Reason for Termination	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Line Reporting Manager
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Salary	Start Date
Weight	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Height	Surname
Marital Status	Nationality
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature

Former Employees

Health Data	
Health Data	
Contact Information	
Contact Details	

Professional Experience & Affiliations	
Trade Union Membership	
Correspondence	
Personal information provided voluntarily	
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Disciplinary Action	End Date
End Date and Reason for Termination	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Line Reporting Manager
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Salary	Start Date
Weight	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Height	Surname
Marital Status	Nationality

Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature

Externals

Contact Information	
Contact Details	
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data At all stages of pre-litigation and litigation, personal data can be included in diverse communications or legal documents sent:

- within the EPO:
- for information and consultation of operational units or staff members involved in the conduct of litigation, on a strict need-to-know basis (Administrative Council Chairman and Secretariat, Office's hierarchy, HR, Employment Law, Boards of Appeal Unit, Conflict Resolution Unit, Ethics and Compliance Unit)
- In case a translation is needed, to Language Services
- In the course of proceedings to decision-making (Administrative Council) and consultative bodies (Appeals Committee)

- possibly outside the EPO:
to external attorneys.

Purpose of sharing Operational units or staff members involved in the conduct of litigation (Administrative Council Chairman and Secretariat, Office's hierarchy, HR, Employment Law, Boards of Appeal Unit, Conflict Resolution Unit, Ethics and Compliance Unit): for fact-finding purposes, information and/or consultation

Language Services: for obtaining a translation.

Administrative Council and Appeals Committee: for the purpose of carrying out certain procedural actions.

Possibly: external attorneys for the purpose of seeking representation or assistance.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Adequacy Decision

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OpenText - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 86

Name Microsoft Office365 applications

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft	

Indra

External processors	
Name Indra	

Description of the processing

Description Office 365 is a cloud-based package of applications (Word, Excel, PowerPoint, Outlook, SharePoint Online, OneDrive, MS Teams, MS Forms and others also listed in the Product Terms, December 01, 2021) provided to users with the aim to offer more flexibility and improve communication, collaboration, as well as the availability of resources.

As mentioned above, the Office 365 package also includes MS Teams, its core features include business messaging, calling, audio and video meetings and file sharing. MS Teams is a cloud-based application to organise virtual meetings and teleconferences both within the EPO and between the EPO and EPO’s stakeholders. The core capabilities in Teams include business messaging, calling, video meetings, and file sharing.

In addition to these core capabilities, MS Teams also allows the recording of virtual meetings and the use of live captions. The use of such features is granted to specific stakeholders in accordance with internal policies on the use of MS Teams. For instance, the possibility of recording a virtual meeting depends on the nature of the meeting and must be authorised by the Data Protection Liaisons (DPLs). Participants will be notified both in the invitation and before the recording is activated that the meeting will be recorded and will be informed about the possibility to object to the recording.

In addition, Office 365 also includes non-optional Connected Experiences which are designed to enable more effective creation, communication, and collaboration.

Personal data is processed, i.e. collected and stored in Microsoft’s cloud servers, for the purpose of providing the above-mentioned services.

Purpose of Processing Microsoft Office 365 applications are used by EPO employees and contractors to fulfil their daily tasks. Within the scope of the present processing operation, PD4.6 Delegated Controller processes personal data for the following purposes: • Delivering MS Office 365 applications and services to the EPO's staff and contractors • Providing end-user support and troubleshooting for Microsoft 365 Office applications and features • Managing content uploaded to Microsoft Office 365 • Managing Microsoft Office 365 settings • Supporting, operating and maintaining the Microsoft Office 365 applications. Microsoft Office 365 apps may be used for a number of different, specific purposes and scenarios, which the present record does not take into account. Delegated Controller BIT PD4.6 is accountable only for the purposes of processing that are stated in the present record. Any EPO Delegated Controller may decide if/when/which Microsoft Office 365 app to use, in order to fulfill own business purposes, tasks and activities. The specific scenarios and purposes - established by a given EPO delegated controller other than BIT PD4.6 - fall into said delegated controller's accountability remit and are described in its related records.

Data Retention At all times during the term of EPO’s contract with Microsoft, EPO has the ability to access, extract and delete the data stored in the applications. Microsoft will retain EPO data that remains stored in the applications in a limited function account for 90 days after expiration or termination of EPO’s subscription so that EPO may extract the data.

After the 90-day retention period ends, Microsoft will disable EPO’s account and delete the EPO Data and Personal Data within an additional 90 days, unless Microsoft is authorized under the contract with EPO to retain such data.

For Personal Data in connection with the applications, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon EPO’s request, unless authorized under the agreement with EPO to retain such data.

EPO specific retention policies:

OneDrive: personal data is automatically deleted from OneDrive one year after the user account has been deleted.

Teams Chats, Teams Channel Messages, One Drive and Sharepoint content are stored until EPO's termination of the contract with Microsoft as explained above. If a Chat or Message in Teams is deleted by a user (or if any content in OneDrive and Sharepoint is deleted by user), then it is retained for one year after the last modification date in an area only accessible by an administrator before a final deletion.

For Teams, the history of phone calls is kept for 90 days and can be seen by administrators; an end-user can only see a 30-day-long own list of own phone calls.

Recordings of Teams meetings made using the Recording feature are retained for a period of three months before deletion unless otherwise defined by the recorder. Recording of Live Teams events are kept for 180 days. Such recordings may be kept for longer than one year depending on the nature of the meeting, whereby the period of retention is defined in accordance with the purpose of the recording. If a recording becomes outdated or obsolete before the end of the retention period it will be deleted. The specific retention period is provided in a dedicated data protection statement and/or disclaimer which is sent with the invitation to the meeting.

For surveys done via Forms: the survey owner is responsible for defining, communicating and manually enforcing the retention he/she has decided.

Data subjects and categories of personal data

Contractors

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Physical and/or Digital Identifiable Assets	
Mobile Device Name	Operating System Version
Workstation's Hostname (Physical or Virtual)	
Sensory and Electronic Information	
Audio Information	Presence Status
Visual Information	
Telephony Interaction Data	
Telephony Session Content	Telephony Session Details
Telephony Session Metadata	
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Language preference (of communication)
Office Location	Room Number
Personal Identification	
Digital signature	First Name
Surname	Picture
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Phone Numbers	Working email address

Device Management Data	
Account ID	Last Logon Time
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Cookie Information	IP Address
Network Interaction History	URL
Website History	
User Account Information	
Account Age	Account Number
Membership Permissions	Ownership Permissions
User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Ports	Registry data
Running Processes	System-, Application-, Security-related Server Logs
Transaction-related Details	Web Servers Logs

Employees

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Physical and/or Digital Identifiable Assets	
Mobile Device Name	Operating System Version

Workstation's Hostname (Physical or Virtual)	
Sensory and Electronic Information	
Audio Information	Presence Status
Visual Information	
Telephony Interaction Data	
Telephony Session Content	Telephony Session Details
Telephony Session Metadata	
Employment Information	
Business Unit Division	Department name and/or number
Job Title Role	Language preference (of communication)
Line Reporting Manager	Office Location
Personnel Number	Room Number
Personal Identification	
Digital signature	First Name
Surname	Picture
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Phone Numbers	Working email address
Device Management Data	
Account ID	Last Logon Time
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Browsing Information	
Browser type	Browser User Agent

Browsing Date and Time	Browsing Time
Cookie Information	IP Address
Network Interaction History	URL
Website History	
User Account Information	
Account Age	Account Number
Membership Permissions	Ownership Permissions
User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Ports	Registry data
Running Processes	System-, Application-, Security-related Server Logs
Transaction-related Details	Web Servers Logs

Externals

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Network/application Interaction Data	
Session content	Session details
Session metadata	
Sensory and Electronic Information	
Audio Information	Presence Status
Visual Information	
Contact Information	
Personal Email	Working email address
Correspondence	

Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Telephony Interaction Data	
Telephony Session Content	Telephony Session Details
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Cookie Information	IP Address
Network Interaction History	URL
Website History	
System Logs	
System-, Application-, Security-related Server Logs	Web Servers Logs

Recipient of the personal data

Recipients of the data Personal data is disclosed on a need-to-know basis to the following recipients:
• EPO staff and external users included in Office 365 applications used for the exchange of information (for instance, the participants to an MS Teams meeting or the sender and recipient(s) of an email exchanged in Outlook).
• EPO PD4.6 , Indra and Microsoft staff involved in the data processing necessary to provide the service.

For Office 365, in principle the majority of the service operations are automated in order to reduce the need for human access.

Microsoft staff does not have standing access to EPO data and any required access is for a limited time. Moreover, Microsoft employs least privilege access mechanisms to control access to EPO data.

Where a virtual meeting is recorded in Ms Teams, the recording may potentially be disclosed to the EPO as a whole, or outside the EPO, depending on the meeting. In either circumstance, the data subject will be duly informed by the meeting organiser of the details of the processing operation.

For surveys/forms/questionnaires organised by an Owner via MS Forms: questions and answers are stored in Microsoft cloud; access to a survey's submitted responses is available to the survey's owners only. In case of anonymous survey, no contact information about the respondent is included in the response. In case of confidential surveys (= non anonymous), the owner has access to the respondent's name, email address, date and time when the respondent opened the survey, and data and time when the respondent submitted the response.

Purpose of sharing In the present processing operation, personal data is shared with EPO staff, contractors and external users in order to enable them to perform EPO tasks and activities.

Personal data is shared with the external processors (Microsoft and Indra) and EPO PD4.6 for the following purposes:
· Delivering MS Office 365 applications and services to the EPO
· Support, operation and maintenance of MS Office 365 applications
· End-user support and troubleshooting for Microsoft Office 365 applications and features “

In addition Indra and EPO PD46 may process personal data for the following purposes:
· Managing MS Office 365 settings
· Security purposes

Microsoft also processes the data for business operations purposes for which Microsoft is a Data Controller: (1) billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and business modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting and compliance with legal obligations. More information on this processing can be obtained in Microsoft’s public documentation

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Protection against malware, login to Azure Active Directory, error analysis, load balancing, diagnostics data, connected experiences, and processing for Microsoft’s business operations

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted on EPO premises, the providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a

privacy and security risk assessment. Any personal data in transit over public networks between the EPO and Microsoft, or between Microsoft data centres is encrypted by default. Personal data as part of any data that are provided to Microsoft by, or on behalf of, EPO through use of the Microsoft 365 services is encrypted at rest. Regarding the implementation of the encryption, Microsoft uses state of the art encryption technologies. Furthermore, Microsoft employs least privilege access mechanisms to control access to personal data which are part of data that are provided to Microsoft by EPO and role-based access controls are employed to ensure that access to such personal data required for service operations is for an appropriate purpose and approved with management oversight. For Microsoft 365 Applications any required access by Microsoft is for a limited time. Microsoft 365 applications implement and maintain multiple security measures for the protection of personal data as part of any data that are provided to Microsoft by EPO through use of the Microsoft 365 services, which encompass the following: organisation of information security (e.g., security ownership, security roles and responsibilities, risk management program), asset management (e.g. asset inventory and asset handling), human resources security (e.g. security training), physical and environmental security (e.g. physical access to facilities, physical access to components, protection from disruptions, component disposal), communications and operations management controls (e.g. operational policy, data recovery procedures, anti-malware controls, event logging), access control measures (e.g. access policy, access authorisation, least privilege, integrity and confidentiality, authentication, network design), information security incident management (e.g. incident response process, service monitoring) and business continuity management. Microsoft also implements and maintain appropriate technical and organisational measures for protection of any other personal data distinct from the one described above, which are described in Microsoft Security Policy. Microsoft 365 applications have been configured to preserve the confidentiality of the information by employing the measures listed above. In addition, anonymous access is not authorised. Any information you add to Microsoft 365, be it via chat, videoconference, or file sharing, will be available only to the specific users and groups indicated in section 4 above. Microsoft 365 applications are certified in several security standards, including ISO27001, ISO 27002, SOC1 Type II, SOC2 Type II and ISO27018 Code of Practice for Protecting Personal Data in the Cloud. Microsoft conducts annual audits of the security of the computers, computing environment, and physical data centres that it uses in processing of personal data. The audits are performed by independent, third-party auditors according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. Personal data is stored in the EU according to the application configuration implemented by the EPO. It may, however, be made available to subprocessors in other countries, depending on

the requirements for maintenance, support or operation of cloud-hosted services, and the availability of this expertise. If access is granted, it is always temporarily and only to the data required for the specific maintenance, support or operation procedure being carried out. The following safeguards are implemented: • In all transfers to third countries, Microsoft uses EU Standard Contract Clauses for data transfer with its sub-processors. • Microsoft requires subprocessors to join the Microsoft Supplier Security and Privacy Assurance Program. This programme is designed to standardise and strengthen data handling practices, and to ensure that supplier business processes and systems are consistent with those of Microsoft. Specific measures relating to the recording of MS Teams meetings: Where a virtual meeting is recorded, participants can limit the processing of their personal data by activating/de-activating their microphone and camera. In addition, where there are legitimate grounds, participants can also ask via the chat feature for the recording to be temporarily suspended so that they can contribute without being recorded.

Data protection statement

Data Protection Statement link internet In progress

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 92

Name Run and participate in electronic procurement procedures

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 47 - Procurement and Vendor Management

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 46 - CIO / BIT

External processors

SAP

External processors	
Name SAP	

DocuSign

External processors	
Name DocuSign	

AI - Administration Intelligence

External processors	
Name AI - Administration Intelligence	

Description of the processing

Description According to the Financial Regulations, purchasing above a certain threshold must be executed using various competitive procedures or tender processes.

While many competitive procedures still use email to obtain offers from potential suppliers, the eTendering suite (Tendering Platform) of tools from Administration Intelligence is used for tender processes as well as some competitive procedures.
Most buyers in Central Procurement have the authorisation to publish tender and procurement procedures using the eTendering Manager.
Potential suppliers register for eTendering to download procurement documents and participate in said tender procedures.
Their accounts are organisation based, that means 1 organisation with n employees.

They upload their questions and/or bids in the Bidding Cockpit and this data is transmitted electronically back to the Tendering Manager for further processing by the relevant buyer in Central Procurement. The bidders receive automatic notifications to their registered email address informing them when they need to log on to the eTendering platform to see the latest status. Data of registered users as well as uploaded questions and bids are stored in a database on the eTendering server hosted by the EPO at their Data Centre in Luxembourg.

Bidders have the possibility to delete their registration if they so wish once the procedure they participated in has been set to completed by the buyer.
Bidders can delete their account only if they are not participant in a running tender. Even if they have been excluded in an early stage of the tender, they cannot delete their account until the tender is closed.

All EPO suppliers have to be registered on the EPO procurement portal which is a cloud-based source-to-pay platform hosted by Ivalua. Companies winning a tender or procedure are requested to register on the procurement portal and enter all their company information including bank details. This information is interfaced to SAP. The corresponding contract will be created and processed in Ivalua. This includes the integration of the DocuSign process for contract signing with a qualified electronic signature by all parties.

Internally data is additionally stored on the w drive for the creation of documents leading to a final version of a set of tender documents, or later for the financial approval forms and assessment and awards reports. After a procedure has been finalised, the resulting contract is also stored on the w drive with all its drafts and approval documentation.

All procedures above €200k are also recorded in "Extend" which is an excel-based file stored on a share drive. This tool is used to report to management and keep track of bigger exercises- The extend file stores all procurement procedures with all details needed to track their life cycle. That includes the description of the procedure, the buyer ID who initiated it, the EPO colleagues involved in its running, the department that requested it, amount and dates for different

Purpose of Processing To inform potential bidders and bidders to log on to the Tendering Platform as updated information requiring their attention or action is available, To keep logs that include user activity (access time, actions, etc.), which could be used to resolve user incidents., To inform EPO buyers that potential bidders have submitted questions, To manage tender/procurement procedures

milestones of the procedure. It also includes data on the participants (external companies) that submitted offers for each procurement procedure and if they were awarded with a contract.
The data is filled in by the buyers and is accessible only to the staff in Procurement. The data from this tool is exported daily to a database to be used for reporting in Tableau.

The reports based on this data are relevant and restricted only to the Finance & Procurement staff together with VP4 management and main business stakeholders. The data in this tool is used as main input (after manual alteration to exclude any sensitive data) for the planned procurement procedures published on the EPO procurement website.

In order to give internal stakeholders access to tender relevant information a baylon database has been created in order to share information on i.e. bids, contract drafts, assessment and award reports etc.
The source to contract part of the electronic procurement process is covered by iValua

Data Retention In eTendering, bidders can delete their company registration if they so wish once the procedure(s) they participated in has been set to completed. Employee information can be deleted at any time as long as there is still one employee registered for participation in an open procedure. User administrator can delete personal data upon request.

Personal data processed by DocuSign will be kept as long as the contract with the provider is in place and feature are available to close users' profiles upon requests. Personal data processed for the verification of the identity in the context of the e-signature are retained for a maximum of 90 days before being erased.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Working email address
Biometric	
Facial Recognition	
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Personal Identification	
Digital signature	First Name

Surname	Signature
User Account Information	
Account Number	Account Password
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	
System Logs	
Audit Logs (a.k.a. Audit Trail)	

Contractors

Contact Information	
Contact Details	Phone Numbers
Working email address	
Biometric	
Facial Recognition	
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Personal Identification	
Digital signature	First Name
Full Name	Surname
Signature	
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	
System Logs	
Audit Logs (a.k.a. Audit Trail)	

Employees

Contact Information

Phone Numbers	Working email address
Biometric	
Facial Recognition	
Employment Information	
Job Title Role	Office Location
Personal Identification	
Digital signature	Signature
User Account Information	
Password	User ID
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	
System Logs	
Audit Logs (a.k.a. Audit Trail)	

Recipient of the personal data

Recipients of the data Participants in the procurement procedure, such as the EPO buyer, (potential) bidder, the EPO business unit receiving the final bid documents.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Binding Corporate Rules, The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) DocuSign - United States, SAP - United States

Reasons for the transfer Service provider processing the personal data outside the EEA

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 94

Name Flu vaccinations campaign

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 423 - HR Essential Services

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

External processors

Griep Vaccinatie Service (GVS)

External processors	
Name Griep Vaccinatie Service (GVS)	

Description of the processing

Description • Registration to the flu vaccination is possible via the EPO online tool for TH and BE staff, via the online booking tool of Helios for Munich staff and in Vienna the appointments are scheduled with the EPO external occupational health physician directly
• Vaccination is administered by the EPO external occupational health physicians in Berlin and Vienna, in The Hague and Munich by the external service providers
• Documents to be filled out before getting the vaccination are the questionnaire on the medical history of the person receiving the vaccine and the consent form.
• These documents are required to ensure safe vaccination and are checked, collected and stored by the medical staff who administered the vaccine.
• Upon request of the vaccinated persons, the medical staff can register the vaccination in their vaccination book

Purpose of Processing The purpose of the processing is to offer vaccination to EPO active staff and their family members in the framework of vaccination campaigns organized by the Office. Vaccination shall happen following the relevant national legislations.

Data Retention Questionnaires are in paper form and are retained according to the following criteria governed by national provisions.
GVS stores the data for a 15 year period.
The OH Physician in Vienna stores the data for 1 year.
The OH Physician in Berlin stores the data for a 10 year period.
Helios stores the data for 10 years.

Data stored in the EPO registration tool is deleted after 1 year.

Data stored in OHS common box is deleted after 5 years.

Data subjects and categories of personal data

Employees

Health Data	
Health Data	
Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Personal Identification	
Date of Birth	First Name
Surname	

Externals

Health Data	
Health Data	
Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers
Personal Identification	
Date of Birth	First Name

Surname	

Recipient of the personal data

Recipients of the data Physical Security is in charge of registering family members entering the EPO building and providing them with a temporary badge.
The health insurance administrator (Cigna) receives an anonymised report for invoicing purposes from Occupational Health Services and it might request the list with the names of those who got vaccinated for control purposes.

The data are not used for any other purposes nor disclosed to any other recipient.

Purpose of sharing Physical Security is in charge of registering family members entering the EPO building and providing them with a temporary badge.
The health insurance administrator (Cigna) receives an anonymised report for invoicing purposes from Occupational Health Services and it might request the list with the names of those who got vaccinated for control purposes.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 95

Name Processing of personal data within the framework of the European and International Cooperation units' tasks, duties and activities

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 51 - Cooperation and Patent Academy

Entity Name - Processor (Entities) DG0 - 02 - Communication, DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

AMEX GBT

External processors	
Name AMEX GBT	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description European Co-operation - D 5.1.1 (EC) is responsible for developing relations and the implementation of the co-operation policy with the member states and the extension states, and promotes the strengthening of the European Patent Network (EPN). Moreover, the directorate maintains the relationships with European Union Intellectual Property Office (EUIPO) and the European Commission.

International Co-operation - D 5.1.2 (IC) is in charge of the Office's bilateral relations with non-

member states, WIPO and international user associations as well as of the multilateral co-operation with the Trilateral and IP5 offices.

For executing the tasks and duties of the EC and IC units, personal data is processed as follows:

1)The EC and IC, store in a European Cooperation Database and in an International Cooperation Database respectively country specific data of the Member States and Non Member States national patent offices (NPO) respectively and additional stakeholders mentioned above, such as country profiles, correspondence, agreements concluded, personal data of EPO's contact persons. The data is based on own research or documents from external sources.

The databases also include personal data of the EPO's contact persons at the respective National Patent Offices (NPOs) and its Heads of Offices, political persons in charge of/responsible for the respective NPO or other persons the Directorate co-operates with from the institutions mentioned above. This data is obtained from the respective NPO and stored upon receipt. Once a contact at the NPO changes, the data of the outgoing person is either destroyed or kept for archival/historic/institutional/accountability reasons, since often EC and IC are requested to give the high management information on contacts which took place and with whom. The same applies with regards to the other institutions mentioned above.

The ECDB and ICDB serve not only as a repository but also as a working DB, i.e. for activities/meetings/trainings/event planning including financial budgeting tied to the Member States and Non Member State's co-operation plans/agreements has been drafted and created therein – linked to a separate area (ICDB-FMCU) monitored by DG5 Operations for the financial processing of invoices.

The ECDB and ICDB further serve as repository of all types of internal statistical data (e.g. EPOQUE Net, FedReg, EPO monthly reports, etc.) and other background information data necessary and required for the purpose of internal documentation preparation for the bilateral co-operation plans/agreements with the Member States, Non Member States and other institutions and the planning of activities, events, high-level meetings, etc.

The ECDB and ICDB which in their present structure have more historical archive function for the European and International Cooperation units respectively are stored in Lotus Notes.

2) Working level data (e.g. invitations by email, correspondence with the NPOs and other relevant institutions etc. are stored in MS Teams or in the EPO's Email system.

3) The EC and IC units liaise with AMEX GBT, to which identification documents (e.g. passport copies) of event participants are sent for the

Purpose of Processing The purposes of the processing is to have an up-to-date and accessible database for staff of Dir. European Cooperation and Dir. International Co-operation only, of the Member and Non-Member States' NPOs relevant data respectively, which enable planning and preparation of activities/meetings/trainings/events, internal documentation preparation for the bilateral co-operation plans/agreements, generating statistical data including financial budgeting., Carrying out the official duties of PD 51, more in particular D511 and D512

purpose of organising a trip (e.g. airplane ticket, hotel) in the context of organising events.

4) It can occur very seldom that an institution (e.g. WIPO) with which the PD51 has a cooperation agreement, requests a bulk of published patent data, which PD51 endeavours to provide. The delivery of such data may involve the use of post services.

Data Retention Data collected by Dir. European Co-operation and Dir. International Co-operation are kept for historical/archival reasons indefinitely, however they are minimized to only what is strictly necessary (name, organisation, position); the rest of the data concerning a data subject such as telephone and email addresses are kept only for as long as the data subject collaborates with Dir. European/International Co-operation.

Financial data of externals such as travel tickets etc will be kept until the end of the audits of the accounting period.

For EPO staff and Contractors, the EPO rules (FinRegs) apply.

Data subjects and categories of personal data

Contractors

Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Contact Details	Emergency Contact Details
Phone Numbers	Working email address
Professional Experience & Affiliations	
CV	Qualifications Certifications
Correspondence	
Personal information provided voluntarily	
Financial	
Bank Account Number	Fund Reservation Requests
Travel & Expense	
Expense Details	Travel Booking Details
Employment Information	
Business Unit Division	Company Entity

Department name and/or number	Language preference (of communication)
Personal Identification	
Full Name	Surname
Nationality	
Education & Skills	
Languages	

Employees

Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Contact Details	Phone Numbers
Working email address	
Building area and site	
Building area and site	
Professional Experience & Affiliations	
CV	
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Travel & Expense	
Expense Details	Travel Booking Details
Employment Information	
Department name and/or number	Language preference (of communication)
Office Location	Room Number
Personal Identification	
First Name	Full Name

Gender	Surname
Nationality	
Education & Skills	
Languages	

Externals

Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Contact Details	Emergency Contact Details
Phone Numbers	Working email address
Professional Experience & Affiliations	
CV	
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Financial	
Bank Account Information	Bank Account Number
Fund Reservation Requests	
Travel & Expense	
Expense Details	Travel Booking Details
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Language preference (of communication)
Office Location	
Personal Identification	
First Name	Full Name

Gender	Surname
Nationality	
Education & Skills	
Languages	
Government Identifiers	
Passport Number	

Recipient of the personal data

Recipients of the data Personal data are only shared on a need to know basis, as follows:
· EPO staff from D 5.1.1 – access to personal data related to European cooperation;
· EPO staff from D 5.1.2 – access to personal data related to International Cooperation;
· Staff from the hierarchical line of D 5.1.1 and D 5.1.2;
· Staff from the Presidential Office;
· EPO staff from all the units involved in the meetings (BIT, Protocol, Communication);
· Microsoft staff;
· Amex GBT staff;
. Physical security (entry controls) responsibility of DG 4
. National patent offices, international organisations and other organisations and associations with which PD51 (D511 and D512) have agreement with.

Purpose of sharing Personal data are only shared on a need to know basis for the following purposes:
· EPO staff from D 5.1.1 – carrying out duties of European cooperation;
· EPO staff from D 5.1.2 – carrying out duties of International Cooperation;
· Staff from the hierarchical line of D 5.1.1 and D 5.1.2 - internal briefings of top management;
· Staff from the Presidential Office - internal briefings of the President;
· EPO staff from all the units involved in the meetings (BIT, Protocol, Communication): arranging for missions, organisation of meetings;
· Microsoft and BIT staff: providing Microsoft services and support;
· Amex GBT staff: for providing the services;
. Physical security for entrance/access controls
. National patent offices, international organisations and other organisations and associations with which PD51 (D511 and D512) have agreement with - for exchange of information and organising meetings in the scope of a cooperation agreements and very rarely for sending published patent data

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation In case of International Co-operation, to Patent Offices outside the EPC contracting states and international organisations (e.g. WIPO)

Transfer mechanism(s) The recipient provided appropriate safeguards, A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities, Public Authorities/Government Bodies, Organisation of an event

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet DPS not yet approved by DPO

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 96

Name House Ban List

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 44 - General Administration

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

External processors

Security Services Contractor at all EPO sites

External processors	
Name Security Services Contractor at all EPO sites	

Description of the processing

Description Facility Management and its EPO Security Sections are in charge of controlling access to the EPO premises in all sites.
As part of the control of access, all visitors are required to register at the entrance of each building by the reception desk. The visitors are required to present a legitimate form of identification and to have a contact person from the EPO who will guide them and accompany them.
In some cases, applying Art. 3 of Circular 380, to protect the interest of the Office, its staff and visitors, Security Sections at each site register individuals who entail a risk for the Office in the so-called House Ban list. The names of individuals to be added to this list are provided to Physical Security, which maintains the list. Those in charge of securing the Office premises at each site are then receiving a notification of the addition of a new name to the list and are also asked to prohibit access to their premises in case the individual will come to visit their site.
In order to register a visitor, employees of the external security contractor first verify that the visitor is not prohibited from accessing to the premises. To do so, they verify their names to see if they are included in the list of individuals who are banned to access the EPO. At the condition that the visitor is not listed and are duly announced by an EPO staff member, they can get a visitor badge and access the premises.
The list is kept in an EPO database (Babylon). Its access is currently restricted by means of a password (Babylon). The folder in Babylon restricted for access to a limited number of staff which roles involve responsibilities linked to the security of buildings.

Data Retention All categories of personal data of the individual are immediately removed from the list as soon as Physical Security has been informed that the house ban has been lifted. In addition, a yearly review is carried in addition to the latter.

Purpose of Processing Personal data is processed according to Art. 3 of Circular 380 , for the purpose of implementing the necessary access control measures for the protection of the EPO staff and their visitors, its information and assets. Persons are banned access to the Office whenever they may entail a risk for their staff, visitors, information or assets.

Data subjects and categories of personal data

Employees

Employment Information	
Business Unit Division	Line Reporting Manager
Office Location	Personnel Number
Personal Identification	
First Name	Full Name

Externals

Personal Identification	
First Name	Full Name

Recipient of the personal data

Recipients of the data EPO Physical Security and Security Contractor staff at all sites.
Heads of Facility Management at all sites and their deputies.

Purpose of sharing Need to know basis.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet The DPS will be available on the EPO website

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 102

Name Onboarding and Offboarding external BIT Staff

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

Entity Name - Processor (Entities)

External processors

SAP

External processors	
Name SAP	

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description Onboarding process
The Contract Managers (EPO Contract Manager or External Contract Managers) are responsible for informing BIT whenever a new contractor will join BIT.
Under the current procedure, an Excel template needs to be completed with all the contractor's details and the EPO Contract Manager information and submitted to Userreg@epo.org.
The request can also already indicate whether hardware equipment will be required (PCs for on-site – VDI for off-site), so no additional separate equipment request is needed. In cases when a contractor has been previously onboarded and there is only a need for an assignment of a PC or Virtual Machine, such request is conducted via the ServiceNow portal.
The UserReg team will take care of verifying the request and, as relevant, register the user (contractor) in FIPS – from where the Windows account and e-mail are generated the following working day. Logging instructions are sent to the EPO Contract Manager, External Contract Manager and designated Line Manager when indicated. For a virtual machine (VDI), login instructions will be sent to the contractor's EPO email address.

Contractors receive EPO access badge with their picture which is made by Service Line (serviceline@epo.org).

Offboarding process
The Contract Managers are also requested to indicate the end-date of the contractor with their initial request. Contractors are flagged (in FIPS) to become "inactive" on that date and will not be able to use their EPO account any longer, unless an extension has been requested. Two weeks after an end-date of a contractor, all his/her hardware/VDI are decommissioned.

Contract extensions or early termination
When the original end-date changes (either it is extended or shortened) it is reported via the excel document (with the contractors details) which is sent again, highlighting the changes."

Data Retention The Excel sheets for the requests are not stored separately.
The userreg@epo.org mails are kept for 6 calendar years to cover the average (framework) contract duration of 5 years.

Contractors and their UserIDs registered in FIPS are kept in line with the retention periods for HR related data in FIPS. The data for external contractors needs to be kept in case of returning contractors – successive contracts – duration, etc.

Purpose of Processing Onboarding and offboarding of external contractors that work for BIT – with the purpose to initiate the process for the creation of their UserIDs, provision them with the necessary hardware and take care of the offboarding when the contractors leave the EPO.

Data subjects and categories of personal data

Contractors

Contact Information	
Working email address	

Employment Information	
Department name and/or number	End Date
Office Location	Personnel Number
Previous Work History	Room Number
Start Date	
Personal Identification	
First Name	Gender
Surname	

Employees

Contact Information	
Working email address	
Personal Identification	
First Name	Surname

Externals

Contact Information	
Working email address	
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data BIT End User Computing
Contract Managers (EPO and External)
Line Managers
Physical Security (via ServiceLine)
HR

Purpose of sharing BIT End User Computing: verification of requests and registering contractors
Contract Managers (EPO and External): responsible for the contracts under which the contractors operate
Line Managers: providing assistance to contractors
Physical Security (via ServiceLine): for making available the EPO physical access badges
HR: keeping an up to date list of former, current and prospective external resources

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) Microsoft - United States, SAP - United States

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Data Protection EU Comm Standard Contractual Clauses

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, Coherence checks are done by UserReg on the input excel files which Contract Manager submits to UserReg, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., Mailbox UserReg@epo.org is accessible only to 4 named staff members in D4634;

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 103

Name Processing of personal data within the framework of approval of formal documentation by the President's Office

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 01 - Chief of Staff, President`s Office

Entity Name - Processor (Entities)

External processors

OpenText

External processors	
Name OpenText	

Description of the processing

Description In the frame of the submission for information or approval process by the President, both referred to as "Note to the President" or "NttP", the President's Office (PO) is entrusted to receive and process, via the CommonLog tool, formal documents and requests submitted by all relevant departments throughout the EPO.

Data Retention The files are subject to an administration retention Time, which corresponds to the President's term of office. At the end of the President’s term of office, all files are transferred to the EPO archives (for permanent preservation, including the personal data concerned).

Purpose of Processing Administrative handling of Notes to the President (NttP) provided by EPO departments to inform or request approval of the President of the Office

Data subjects and categories of personal data

Employees

Health Data

Health Data	
Contact Information	
Contact Details	
Professional Experience & Affiliations	
Qualifications Certifications	
Correspondence	
Additional Information which might be provided in the course of exchanges	
Background Checks	
Criminal Records	Reference or Background Checks
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Disciplinary Action
End Date and Reason for Termination	Exit Interview and Comments
Grade	Grievances and Complaints
Job Application Details	Job Title Role
Line Reporting Manager	Office Location
Performance Rating	Personnel Number
Previous Work History	Rewards history
Start Date	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Marital Status
Nationality	
Education & Skills	

Academic Transcripts	Education and Training History
Educational Degrees	Languages

Prospective Employees

Health Data	
Health Data	
Contact Information	
Contact Details	Personal Email
Phone Numbers	
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
Background Checks	
Criminal Records	Reference or Background Checks
Employment Information	
Contract Type	Job Application Details
Job Title Role	Military Status
Previous Work History	Start Date
Personal Identification	
Age	Date of Birth
First Name	Full Name
Gender	Surname
Marital Status	Nationality
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages

Former Employees

Contact Information	
Contact Details	Personal Email
Employment Information	

Appeals Records Information	Company Entity
End Date and Reason for Termination	Personnel Number
Previous Work History	
Personal Identification	
Age	Date of Birth
First Name	Full Name
Gender	Surname
Marital Status	Nationality

Externals

Contact Information	
Contact Details	Personal Email
Phone Numbers	
Professional Experience & Affiliations	
Political Affiliation and Activities	Professional Memberships
Qualifications Certifications	
Employment Information	
Company Entity	Job Title Role
Personal Identification	
First Name	Full Name
Nationality	

Recipient of the personal data

Recipients of the data The NttP (and accompanying documents) containing all the types of personal data (of staff and/or externals) is submitted together with the personal data of the responsible sender(s) to the President via the Common Log. Before reaching the President, the NttP is usually subject to a consultation process which make the data accessible for comments, contributions and/or pre-approval by relevant stakeholders in the EPO and staff working in the PO on a need to know basis.	**Purpose of sharing**

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors) OpenText - United States

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 120

Name Study on European Patent Applications to produce statistics on the gender of inventors.

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 012 - Chief Economist

Entity Name - Processor (Entities)

External processors

Externals consultants of the Universities of Bordeaux and Southampton

External processors	
Name Externals consultants of the Universities of Bordeaux and Southampton	

Description of the processing

Description The study is organised by the EPO to produce statistics on the gender of inventors listed in European patent applications. While most of the study is based on EPO's public database PATSTAT, this database does not yet include complete data on patent applications field with EPO in 2020 and 2021.

In order to also enable the production of gender statistics for 2020 and 2021, the EPO will provide the contractors with a dataset extracted from EPASYS including the name, surname, and country of residence as well as a randomly generated identifier for all inventors of European patent applications filed at the EPO in 2020 and 2021.

Using this dataset, the contractors will use a predefined algorithm to attribute a gender to these inventors. As a next step they will delete the personal data (names, surnames and country of residence) from the dataset before sending it back to the EPO.

The dataset with gender data will then be matched by the EPO with the respective patent applications. EPO will then use the matched dataset to produce a statistical analysis of the share of women among inventors of inventions for which patent applications were filed at the EPO in 2020 and 2021.

The final report without reference to individual personal data may be published.

Data Retention The personal data (names, surnames and country of residence) received and processed by the contractors will be deleted by the contractors prior to sending back to EPO the results of the algorithmic gender attribution.

- The personal data (names, surnames and country of residence) received and processed by the contractors will be deleted by the contractors prior to sending back to EPO the results of the algorithmic gender attribution.

- The gender data and statistics will be kept by CBA and the CEU data stored in CBA database is kept for the maximum period of 12 months after the study and then deleted.

Purpose of Processing Statistical study on the gender of inventors listed in European patent applications. In order to enable the production of gender statistics for 2020 and 2021, the EPO will provide the contractors with a dataset extracted from EPASYS including the name, surname, and country of residence as well as a randomly generated identifier for all inventors of European patent applications filed at the EPO in 2020 and 2021. Using this dataset, the contractors will use a predefined algorithm to attribute a gender to these inventors. As a next step they will delete the personal data (names, surnames and country of residence) from the dataset before sending it back to the EPO.

Data subjects and categories of personal data

Externals

Employment Information	
Office Location	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data N/A

Purpose of sharing

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet The link on the EPO webpage will be provided

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 122

Name Learning Management System

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 421 - Talent Management

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

External processors

SAP

External processors	
Name SAP	

MST Company

External processors	
Name MST Company	

Description of the processing

Description EPO Talent Academy uses internal systems, external online learning platforms and any other service provider for talent development activities. These systems and platforms process personal data of staff members.

A digital platform known internally as iLearn (and built on SAP SuccessFactors technology), facilitates the management of the talent development activities of the employees, creating the learning catalogue (trainings, e-learning, coachings which could be provided by external contractors whom will have access to data if the case may be), promoting courses, events, collecting the learning history of the employees, evaluating quality and effectiveness of the services for the continuous improvement and development of the learning activities. iLearn is, consequently, the Learning Management System for the organisation.

iLearn makes the above possible as portal for any employee to access information on diverse learning resources and provides access to the external online learning platforms (LinkedIn Learning, Udemy for Business, Coursera, Udacity). A dedicated record of processing activities covering these online external learning platforms is available.

Personal data are processed for the following purposes:

• To plan and organise training activities.
• To create a training history log for EPO staff.
• To issue certificates of participation for the different training courses.
• To collect feedback from participants so that the EPO Talent Academy can deliver better and more effective development activities, according to staff needs and knowledge as well as the skills necessary for their job.
• To evaluate via quizzes, confidence surveys and assessments, the ability of participants to apply the new skills learnt in the development activities.
• To keep logs that include user activity (access time, actions, etc.), which could be used to resolve user incidents.
• Personal data is sometimes collected to create user accounts for online learning platforms or made available to service providers of talent development activities for organisational purposes.

Purpose of Processing To issue certificates of participation for the different training courses., To plan and organise training activities., To keep logs that include user activity (access time, actions, etc.), which could be used to resolve user incidents., To collect feedback from participants so that the EPO Talent Academy can deliver better and more effective development activities, according to staff needs and knowledge as well as the skills necessary for their job., To evaluate via quizzes, confidence surveys and assessments, the ability of participants to apply the new skills learnt in the development activities., Personal data is sometimes collected to create user accounts for online learning platforms or made available to service providers of talent development activities for organisational purposes., To create a training history log for EPO staff.

Data Retention Any personal learning information will be kept during the period of active employment of the employee.

EPO Talent Academy will use course completion data for reporting on talent development activities. This information will be retained for 5 years. Service providers will be instructed to delete the data retained related to usage by EPO staff member on finalisation of the relationship with the EPO.

Personal data will be kept only for the time needed to achieve the purposes for which it is processed.

Data subjects and categories of personal data

Employees

General	
Personal Information in SAP	
Contact Information	
Contact Details	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Ratings
Social learning inputs	
Examination content data	
Examination marks	Examination result
Employment Information	
Business Unit Division	Department name and/or number
Grade	Job Group
Job Title Role	Language preference (of communication)
Personal Identification	
First Name	Full Name
Surname	

Education & Skills	
Education and Training History	

Externals

Contact Information	
Contact Details	

Recipient of the personal data

Recipients of the data Personal data are disclosed to the following recipients:

- EPO Talent Academy staff involved in the administration of talent development activities has access to the personal data of all EPO staff members that is available via SuccessFactors LMS
- iLearn administrator in EPO Talent Academy: Creation, administration and maintenance of basic learning elements (courses offered, development programmes, catalogues, assignment profiles), creation and editing of surveys, recording learning events, assignment and registration of staff to courses, creation of content in the system, creation and access to learning reports, allocation of coach to coachee, visualising staff member's learning history
- Line managers have access to the learning history of their direct reportees via reporting functionalities in iLearn (including all mandatory online learning courses, e.g. those that are part of a staff member development plan) to support the staff member's professional development
- Instructor: View list of courses authorised to teach, view lists of past and upcoming learning events where the instructor is involved, view list of participants to his/her learning events, record attendance to his/her learning events
- Learning Consultant & HRBP: View information about staff enrolment and progression within a development programme, view learning history for staff members, view external requests (participation to an external conference)
- BIT Department, as an internal processor in the role of application manager, has access to the data in iLearn - To support line managers and staff with regard to professional development
- Coach: View list of past and future assigned learning events for coachee, see results of coachee’s assessments, complete coachee’s version of confidence survey to provide effective coaching
- MST company, Munich (Germany) - External company that provides SF Learning administration as part of the EPO externalisation project
- Service providers of training activities, including companies that support the EPO Talent Academy

Purpose of sharing EPO Talent Academy - For administration purposes.
Line Managers - To support personal development of their staff-
EPO BIT Department - In the role of application manager.
Instructors, coaches - To provide the service
Learning consultants and HRBPs - to support them in their functions
MST - To provide the service

Service Providers of training services - To provide the service
Online external learning platforms - To provide the service

See additional details below:

- EPO Talent Academy staff involved in the administration of talent development activities has access to the personal data of all EPO staff members that is available via SuccessFactors LMS
- iLearn administrator in EPO Talent Academy: Creation, administration and maintenance of basic learning elements (courses offered, development programmes, catalogues, assignment profiles), creation and editing of surveys, recording learning events, assignment and registration of staff to courses, creation of content in the system, creation and access to learning reports, allocation of coach to coachee, visualising staff member's learning history
- Line managers have access to the learning history of their direct reportees via reporting functionalities in iLearn (including all mandatory online learning courses, e.g. those that are part of a staff member development plan) to support the staff member's professional development
- Instructor: View list of courses authorised to teach, view lists of past and upcoming learning events where the instructor is involved, view list of participants to his/her learning events, record attendance to his/her learning events
- Learning Consultant & HRBP: View information about staff enrolment and progression within a development programme, view learning history for staff members, view external requests (participation to an external conference)
- BIT Department, as an internal processor in the role of application manager, has access to the data in iLearn - To support line managers and staff with regard to professional development
- Coach: View list of past and future assigned learning events for coachee, see results of

in the administration of learning activities, as well as companies that provide access to their online learning platforms as part of a contractual relationship with the EPO have access to personal data on a strictly need-to-know basis.

Data will only be shared with authorised persons responsible for the corresponding processing operations. Data is not used for any other purposes or disclosed to any other recipients.

coachee's assessments, complete coachee's version of confidence survey to provide effective coaching
- MST company, Munich (Germany) - External company that provides SF Learning administration as part of the EPO externalisation project
- Service providers of training activities, including companies that support the EPO Talent Academy in the administration of learning activities, as well as companies that provide access to their online learning platforms as part of a contractual relationship with the EPO have access to personal data on a strictly need-to-know basis.

Data will only be shared with authorised persons responsible for the corresponding processing operations. Data is not used for any other purposes or disclosed to any other recipients.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors) SAP - United States

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 125

Name Fitness & Vitality Service

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 422 - HR Customer Engagement

Entity Name - Processor (Entities) DG4 - 44 - General Administration

External processors

High Five Health Promotion B.V

External processors	
Name High Five Health Promotion B.V	

Description of the processing

Description Steps of the Procedure

In order to use the fitness services provided by High Five, the staff member has first to register in the High Five portal (using the High Five Connect application) and become a member.
There are two kind of services.

1. Fitness services provided at the EPO premises
This service is for all staff assigned to Munich Isar and PH buildings and The Hague buildings.

1.1. Users of the fitness services are required to undertake an induction training with the High Five trainer scheduling an appointment via the booking tool.
1.2. During the induction training, users are also introduced with the functionalities of the High Five Connect application a hub where users can manage memberships, schedule bookings, track progress, join the health & wellbeing community and maintain contact with High Five professionals
1.3. The only personal information of the users that High Five shares with the EPO is the list with

the names of the members. This list is regularly sent by High Five to the EPO Security Services in order to manage the access rights to the fitness rooms via the EPO personal badge.
1.4. The Security Services and High Five will provide Health and Safety department with anonymous aggregated data on the usage of the service.
1.5. Services that are free of charge
As long as corona measures are maintained: online courses and online one-to-one consultations with a fitness expert
Use of the on-site gyms in Munich (Isar and PschorrHöfe) and in The Hague, induction by the fitness trainer
Via High Five Connect app: online courses, fitness consultations, fitness community, online training plans
1.6. Services that are not free of charge
On-site classes, personal trainer, physiotherapy, lifestyle coaching
1.7. If you leave the Office or if you decide to cancel your subscription, please contact High Five (fitnessepo@highfive.fit).

2. Membership at external fitness clubs
This service is for staff assigned to Munich Haar building, Berlin, Vienna and Brussels.
2.1. Membership is only possible in external fitness clubs that have been agreed between EPO and High Five (see the list in the dedicated intranet page of the Health & Safety department)
2.2. When staff register for this service in the online tool, they are automatically informed that their name will be shared with the fitness club and the Health and Safety department for auditing reasons
2.3. High Five share the names of registered staff with the external fitness club for membership and invoice purposes.
2.4. High Five share the names of registered staff with Health & Safety department for audit and invoice purposes.
2.5. Services that are free of charge
As long as corona measures are maintained: online courses and online one-to-one consultations with a fitness expert
Fitness membership in external local gyms
Via High Five Connect app: online courses, fitness consultations, fitness community, online training plans
2.6. Services that are not free of charge
Check-up, personal trainer, beverages, supplements, massages
2.7. As the High Five and the external local gyms run totally cashless, when registering, you may be asked to provide your back account. You will be charged only if you book/buy services/products not covered by your membership or if you benefit, as family member, external or retired staff from discounted rates.
2.8 If you leave the Office or if you decide to cancel your subscription, please contact High Five (fitnessepo@highfive.fit). Cancellation from external gyms has to be communicated to High Five one month in advance.

Purpose of Processing The EPO commits to provide its staff members with services that are directed at maintaining a healthy lifestyle. This service targets the physical and mental health of all our staff members and provides a space where healthy habits can be encouraged by professional staff of the external providers.

Data subjects are:
- Employees, Contract agents and their family members
- Pan-European Seal Program trainees

The following data types may be processed.
A) Data accessible by EPO and the external service provider
• Identity data – Name, Date of birth, Gender, personal ID number, place of work
• Contact data – work place, E-mail address, Phone number
B) Data accessible by the external service provider only
• Activity data – Visit history, bookings, training schedule
• Payment data – Banking details, payment history, invoices
• Health data – Weight, Blood pressure, Height, Pre-existing conditions, Information regarding nutrition

Data Retention Processes are set up to guarantee the following retention periods:

- In Virtuagym – HighFive Connect member data will remain until manually deleted by High Five or 1 year after cancelation of the contract if the account is no longer in use
- Due to tax legislation High Five will need to store payment data (invoices) for a period of maximum 7 years
- In Technogym Wellness Cloud, the data will be kept for 12 months after membership cancelation. Processes will be set up to guarantee these retention times.

Data subjects and categories of personal data

Employees

Health Data	
Health Data	
Contact Information	
Contact Details	Home Address
Phone Numbers	Working email address
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	
Employment Information	
Business Unit Division	Office Location
Personnel Number	Weight

Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Height	Surname

Externals

Personal Identification	
Full Name	

Former Employees

Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data The recipients of data are:
1. High Five Health Promotion B.V and sub-processors
2. Facility Management- Security
3. Health & Safety department

Health & Safety may have access to aggregated data on the use of the service.

The data are not used for any other purposes nor disclosed to any other recipient.

The external fitness gyms receive the personal data in their role of data controllers of the employee's personal data for all the services they provide.

Purpose of sharing Processor: High Five Health Promotion B.V

Sub-processors:
- Technogym S.P.A (Italy) for training data (Biocircuit training data).
- Digifit B.V (Netherlands) (publisher of Virtuagym) for administration, booking, member portal tool and back-up.
- Hestronic (Netherlands) for IT support.
- Severius (Netherlands) for Hosting
- Microsoft (Netherlands) for Communications with members.

Internal processors:
- Health & Safety department for auditing purposes (check that the persons applying for membership in the external fitness club are EPO staff members)
- Facility Management-Security for the management of the access rights to the fitness rooms via the EPO personal badge.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures	EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 126

Name EP Full Text for Text Analytics

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 54 - Patent Knowledge

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

Microsoft

External processors	
Name Microsoft	

Google

External processors	
Name Google	

Description of the processing

Description The European Patent Office (EPO) distributes a bulk data set consisting of titles, abstracts, descriptions, claims and search reports of EP publications that is based on input data which is collected from the Patent Grant Procedure. The collected input data is used to create reformatted, and repackaged data sets for public distribution. This data is in text format potentially addressing specific user categories who wish to conveniently load the data into their own systems.

The packaged data is made available to the public via the Google Cloud platform.

The cloud platform provider makes service usage data available to the EPO. This service usage data can be analysed within the EPO or using the cloud service provider supplied tools. Data are not anonymised when used for interaction with users for support and service delivery management relating to service usage.

Data Retention The EP publications are public data, therefore the data not deleted.
User data is retained for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore.

Purpose of Processing Distribution of the EP data to the public intended for text analytics, Analytics and ensuring correct service functioning

Data subjects and categories of personal data

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
User Account Information	
Account Number	Third-party User Identifier
User ID	

Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
User Account Information	
User ID	

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Knowledge, BIT, DG1 and senior EPO management (CILO, VP5 Office, President Office, CGS, MAC), and Google as external processor.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation The published data are publicly accessible.

Transfer mechanism(s) Data Protection EU Comm Standard Contractual Clauses, A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, The patent record content is made available to anyone world-wide.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet Will be published on EPO web site once available.

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 127

Name Open Patent Services

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 54 - Patent Knowledge

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description The European Patent Office (EPO) provides Open Patent Services (OPS) which is a web service that provides access to the EPO's patent data collections.

The data made available via the OPS service is extracted from the EPO's patent procedure related information collections and the EPO's world-wide patent related data collections and databases.

Users may access the data without user credentials up to certain usage thresholds. Beyond the fair use threshold, payment is required.

Registered users are granted free access to a specific volume of data up to a certain ceiling defined in the OPS terms and conditions.

Registered users willing to pay for more substantial volumes of data can record billing contact details and apply for access to higher volumes of data in the form of a yearly subscription.

The subscription and payment are in scope of the record Patent Knowledge Webshop

Users may also be contacted for service delivery (support) related issues.

Additional end user information is collected for analytics purposes in order to ensure efficient delivery of the service.

Data Retention User data is retained for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore (e.g. cancellation of a subscription).
Technical service access data can be retained for up to 7 years in order to analyse usage patterns.
Information contained in the patent records is public data which is never deleted.

Purpose of Processing Usage analytics., Communication with users., Access management., Deliver access to OPS.

Data subjects and categories of personal data

Externals

General	
Any other information	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Contact Details	Country
Mobile Phone Number	Phone Numbers

Private Phone Number	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Office Location
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
Personal Identification	
Digital signature	First Name
Full Name	Gender
Surname	
User Account Information	
Account Age	Account Number
Account Password	

Employees

Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Knowledge, BIT, DG1 and senior EPO management (CILO, VP5 Office, President Office, CGS, MAC).

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation The published data are publicly accessible.

Transfer mechanism(s) The recipient provided appropriate safeguards, A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, The service is intended to deliver patent data to world-wide users.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet Will be made available after DPO review of this record, and include link to: ....

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 129

Name Post grant contact management

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 54 - Patent Knowledge

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description A list of contact persons at national patent offices in Contracting States are maintained for the purpose of administering Postgrant Validations team activities and communication with respect to monitoring Article 39 EPC – Payments by the Contracting States in respect of renewal fees for European patents.

The National Patent Office contact persons provide EPO with their contact details.

The contact list is stored on EPO internal storage systems and the communication is carried out using MS Outlook, in the PostGrant@epo.org shared mailbox.

Only patent numbers are used to identify patents during the communication.

Purpose of Processing Communication with contacts from national patent offices in contracting states with respect to monitoring Article 39 EPC

Data Retention Contact details are kept for maximum 7 years after the representatives are no longer allocated to this task by the respective National Office. If considered appropriate, it is also deleted if it can reasonably be expected that there is no operational need anymore.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Phone Numbers
Working email address	
Employment Information	
Job Title Role	
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data Personal data are only shared on a need to know basis with EPO employees undertaking relevant activities.

Purpose of sharing Personal data are shared in order to contact the designated representatives within the National Patent Offices in contracting states with respect to monitoring Article 39 EPC.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet tbd

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 134

Name Official Publications

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 54 - Patent Knowledge

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

Acolad

External processors	
Name Acolad	

Description of the processing

Description The European Patent Office (EPO) has processes for collating and assembling various publications required or closely related to the European Patent Convention, including:

- The Official Journal - source of official information and general notices from the EPO, and of other information relevant to the EPC or its implementation.

- EP Bulletin - regular EPO publication containing bibliographic data, as well as data concerning the legal status of European patent applications and patents.

- Legal Texts: e.g. European Patent Convention

- EP Patent documents (A & B)

- EP Register - the most complete and up-to-date source of publicly available procedural information on European patent applications as they pass through each stage of the granting process.

- EP file inspection - the files relating to European patent applications and granted patents, and to international applications under the PCT for which the European Patent Office acts as a designated or elected Office, are available for inspection online, free of charge, via the European Patent Register.

Personal information of the EPO staff involved in the preparation and processing of content is processed.

Data Retention Information contained in the patent records, and other publications covered by this record, is public data which is never deleted.

Purpose of Processing Preparation of Official publication content., Making Official publication content available to the public.

Data subjects and categories of personal data

Externals

General	
Input provided during the deliberation and decision-making process	
European Patent Register Data	
Data provided by the data subjects	
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Knowledge, BIT, DG1, EPO Legal Services, EPO Boards of Appeal and senior EPO management (CILO, VP5 Office, President Office, CGS, MAC).

Purpose of sharing The legal text data are shared with DG1 to upload into their Single Legal Source (SLS) tool.

The source data for Bulletin processing are shared with D5411 and D5413 for their own processing requirements (e.g. Bulletin Search, Bulk data products).

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation The published data are publicly accessible.

Transfer mechanism(s) A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer The service is intended to prepare and distribute data to world-wide public users.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet Will be made available after DPO review of this record, and include link to: ....

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 137

Name Federated Services

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 54 - Patent Knowledge

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

Not Applicable

External processors	
Name Not Applicable	

Description of the processing

Description The European Patent Office (EPO) offer services to end users that combine inputs collected from distributed patent process related sources (e.g. National Patent Offices) into a combined view. This record relates only to the processing done by the EPO after receipt of data from the distributed sources.

The services concerned include:

- Global Dossier - single-point access to dossier content (file inspection) of patent documents from numerous intellectual property offices, including the IP5 offices. The file content and their translations are made available to the EPO by Global Dossier partner offices.

- Federated Register - single point of access to post-grant bibliographic and legal status information on European patents. It is available free of charge.

Additional end user information is collected for providing alerts and for analytics purposes in order to ensure efficient delivery of the service.

Data Retention User data is retained for up to 7 years after it can be reasonably expected that there is no immediate operational need anymore (e.g. cancellation of a subscription).
Technical service access data can be retained for up to 7 years in order to analyse usage patterns.
Information contained in the patent records is public data which is never deleted.

Purpose of Processing Analytics and managing service delivery., Combining patent process related information from multiple patent offices into a single representation.

Data subjects and categories of personal data

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Contact Details	Country
Personal Email	Phone Numbers
Working email address	
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Employment Information	
Company Entity	Language preference (of communication)
Browsing Information	
Browser type	Browsing Time
Cookie Information	IP Address
Network Interaction History	Website History
Personal Identification	
First Name	Surname
User Account Information	
Account Age	Account Number
Account Password	User ID

Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Former Employees

Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications

Recipient of the personal data

Recipients of the data The patent record content can be made available to anyone who uses the service. These users may be world wide.

Where necessary to perform its tasks, non-patent personal data may be shared on a need-to-know basis with staff undertaking duties in the following areas of the EPO: Patent Knowledge, BIT, DG1 and senior EPO management (CILO, VP5 Office, President Office, CGS, MAC).

Purpose of sharing

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation The published data are publicly accessible.

Transfer mechanism(s) A derogation in accordance with Art. 10 DPR

Reasons for the transfer Public access to service content.

Derogations Art. 10 DPR The transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular case

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet Will be made available after DPO review of this record, and include link to: ....

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 148

Name Workflows in the Patent Workbench

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG1 - 1 - Patent Granting Process

Entity Name - Processor (Entities)

Description of the processing

Description The following generic task workflow covers the Search, Examination and Opposition workflows, as well as actions specific to Formality Officers and to the Quality Auditors. Specificities of each workflow is detailed in the next section.

GENERIC TASK WORKFLOW:

1. An event (Muse, online filing, answer from the applicant, PWB action, ...) automatically triggers an action task creation in the PWB and provides data to the PWB.

2. PWB then automatically assigns the action task to an Examiner or a Formality Officers whose duty is to perform an action.

3. The action is manually performed by the Examiner or Formality Officer either in tools outside the PWB or directly within the PWB. The outcome of the action is the generation of a document or a set of documents stored outside the PWB. Completion of the action is automatically logged in the PWB and triggers step 4. for examiners' actions and step 7. for Formality Officers' actions.

4. The PWB automatically circulates a review task to Review Members in charge of the review task who have the duty to review the action performed in step 3. Each of them has to log manually whether the action is approved or not in the review task, and can optionally enter comments that are visible for all members involved in step 3

to 6b.

5. If any of the members in charge of the review task of Step 4. logs manually a non-approval of the action, this triggers the process to returns automatically to step 2. This loop is repeated as many times as necessary as long as a non-approval is logged manually by any members in charge of the review task of step 4.

6. If all members in charge of the review task log manually the approval of the action, then the action task and review tasks are automatically closed and archived, and either

6a. the formality Officers performs manually a further processing of the action and action documents with a tool outside PWB; or

6b. for enhanced flows, PWB directly generates the documents, sends them to the applicant and updates the legacy tools.

7. The action task performed by Formality Officers in step 3 is closed and archived, ...
7a. automatically when the Formality Officer terminates the actions in PWB; or
7b. manually by an employee of the Finance department, after the Formality Officer has manually transmitted (=Trigger) the action to the finance department through PWB.

PROCESSING PERSONS IN SPECIFIC WORKFLOWS

The Review Members of steps 4-6 for tasks performed by Examiners in step 3. are:
- For Search actions: the Line Managers and their deputies, Formalities Officers and eventually the Chairperson in case of positive search

- For summons to oral proceedings in examination: The Examining division, the Line Managers and their deputies, Formalities Officers.

- For minutes of Oral proceedings: the Chairperson, the Line Managers and their deputies, Formalities Officers.

- For examination IGRA (Intention to GRAnt) and Refusals: The Examining division, the Line Manager and their deputies, Formalities Officers, and eventually Quality Auditors* for IGRAs.

- For enhanced flows (eComm, ePrep, eTel, eOR9C): The Examining division, the Line Manger and his deputies (and optionally Formality Officer if the automatic process).

- For other examination Tasks: The Line Manger and his deputies, Formality Officers.

- For tasks of the opposition division: The opposition division, the Line Manager and his deputies, Formality Officers.

- For all actions, there is the possibility to add a

Purpose of Processing The purpose of this processing is to ensure a seamless workflow and communication between the EPO employees involved in the patent granting process. Processing contact data is needed to perform the routing of tasks between employees involved in the patent granting process and enable communication between them. Processing Log data and comments is needed to enable communication completeness and timeliness of the task execution. Moreover, user might need to retrieve previous comments when checking again the same task. (Legal Basis: see document “New data protection rules – alignment with the patent grant procedure”)

Legal Member (DG5) in the review process.

* Quality Audit: for IGRA review, after the Line manager has approved the IGRA task, and before the Formality Officers perform their review, actions are randomly sampled and fill a buffer from which Quality Auditors can select a task. The Quality Auditor has access to all data in PWB and can interact with the division exclusively. Discussion between the quality auditor and the division happens outside PWB and no information is shared with the line manager. Only Formalities Officers can retrieve the information that the file has been sampled for the DQA checks.

No review process is in place for actions performed by Formality Officer in steps 3 and 6-7a.

Software and Databases involved in the Workflow

- Steps 1, 3 and 7: Triggers and data from the external events or previous step events are collected in Kafka with a retention time of 7 days.
- Steps 1-7b: All data about the task and its processing steps (including userID, logs and comments) is processed by the Camunda Process Engine and stored in the Mongo Database. There is one specific Process Engine and one specific Mongo Database for each of these processes: Search, Examination and Opposition. Retention time: unlimited.
- Steps 1-7b: status and history of the task is visible in the PWB for all involved employees (examiners, LM, FO) for 30 days after completion of the task. Retention of these history data is in “Elastic Store” and limited to 30 days after completion of the task.

Data Retention Retention Period:

For Kafka: 7 days
For the Process Engines and Mongo DB: unlimited (legal basis: see document “New data protection rules – alignment with the patent grant procedure”)
For the Elastic Store : 30 days

Data subjects and categories of personal data

Employees

Network/application Interaction Data	
Session details	
Contact Information	
Contact Details	
Correspondence	

Personal information provided voluntarily	
Employment Information	
Business Unit Division	Job Title Role
Line Reporting Manager	
Personal Identification	
Full Name	
User Account Information	
User ID	

Externals

Network/application Interaction Data	
Session details	
Contact Information	
Contact Details	
European Patent Register Data	
Data provided by the data subjects	
Correspondence	
Personal information provided voluntarily	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data EPO employees involved in the processing steps 1 to 7 will have access to the data during the task processing, and in their history function for 30 days after the task has been terminated.
Line managers + deputies will have access to the data during the task processing, and in their history function for 30 days after they terminate the task.
IT administrators have access to all data for maintenance and support.
EPO Service Line internal employees have access to the PWB tool for technical support.
A daily snapshot of the Camunda Process Engines for Search and Examination is copied by department 4612 (Business Analytics CoE) in the Data Warehouse, comprising all data except the comments/notes of the users. No manual nor automatic analysis processing of the captured data is performed by department 4612. These data can be accessed for analysis purpose by users in Dir. 141 (Business Analysis and Planning) and department 1341 (Quality and Risk Analysis).

Purpose of sharing Personal Data are processed for following persons:
DG1 examiners, DG5 Legal member, DG1 Formalities Officers, line manager
Data from the applicant and/or its legal representative.
All processed data are business related and contain no sensitive personal data.
Moreover, data relating to the applicant, the legal representatives and the identity of the examining division members are public data for the patent grant process.
Processed data:
Name of the applicant
Links to the action document(s) which includes eventually contact data about the applicant, employees of the applicant, legal representative of the applicant, or professional contact data of the EPO employee.
First and last name, userID, Team, Directorate and role of the EPO employees involved in the processing steps 1 to 5d, as well as the name of their line managers and directors.
Logging date/time, Approval/non-approval logs, and comments of EPO employees involved in the processing steps 1 to 5d.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet VP1 intranet homepage (link will be provided).

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 157

Name International Women's Day event

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 02 - Communication

Entity Name - Processor (Entities) DG4 - 43 - Welfare & Remuneration

External processors

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description For the organisation of the panel discussion of the International Women's day event, Principal Directorate Communication (PDComm) process personal data to select the panellists, collect testimonials from EPO employees and organise the event.

The gathering of personal data for the selection of panellists is carried out as follows:

1) By inviting external possible speakers, who may be either former panellists in any EPO event (of whom the EPO already have the contact details) or new speakers proposed internally, and whose email address is published on the internet, or
2) By organising an internal call for panellists in which the EPO employees complete a MS form on a voluntary basis. The personal data provided in the form by EPO applicants are deleted once the event has taken place, thus ensuring their replacement in case of urgent need.

The gathering of personal data when collecting testimonials is done through a call for interest organised directed towards EPO employees. The video testimonials are sent directly by the data subjects to the Diversity&Inclusion team (internal data processor), and shared via email with PDComm for editing and publication on the different EPO's internal and external channels. Once the testimonials are edited, the email address of the data subject (as all as other personal data which is not included in the testimonial) is deleted. Only the audio-visual material published on the EPO's internal and external channels remain available.

In order to organise the event, the e-mail addresses of the panellists are processed in order to invite them to the rehearsals and the event.

As for non-panellists (i.e. attendees) they may join the event without prior registration, via a landing page specifically created for it by an external provider, via LinkedIn, Facebook or YouTube. In order to allow individuals to ask questions, the EPO uses the platform Slido. Data subjects can choose directly on Slido whether their questions, comments and/or opinions are posted to the event publicly or anonymously. Additional anonymous data such as numbers of viewers is collected by the EPO for statistical purposes.

Since the event is recorded, audio-visual data of the panellists are processed, and disclosed to the general public along with the video testimonials provided by EPO employees.

Finally, to promote the event, the organisers may process personal data such as e-mail addresses stored in the EPO database.

Purpose of Processing Coordinating any required follow-up activities., To organise the event and select and support the panellists on the preparation of their presentation., To allow you to join the event through the different platforms in which the event is streamed. For that purpose, links to the different platforms will be provided to the public. No registration is needed., To promote the EPO's contribution through its social media networks by publishing the recorded panel discussion and the EPO employees' video testimonials collected in advance.

Data Retention Personal data processed by the data controller or the service providers under its supervision are generally stored for the period of time necessary to achieve the purpose for which they have been processed.

The following time limits for storing the data apply in the context of the call for panellists organised for the EPO employees:

For successful candidates: personal data necessary for the preparation of the event, such as email address and answers and motivations will be deleted as soon as the event takes places.

For non-recruited candidates, data is kept until the event is held to guarantee a replacement, in case a panellist informs us of his/her unavailability at the last minute.

Regarding the data collected by the data processor providing the landing page for individuals to attend the event, once each event ends, the recording as soon as it is delivered to the EPO. Regarding the rest of the data, it is deleted within a period of 3 months.

Regarding the video testimonials provided by the EPO employees, PDComm will store and process the data on its internal databases until the video testimonials are edited for the event and published on the EPO's internal and external channels. After that, the no necessary data is deleted and only remains what is published on the EPO's internal and external channels, that means, the personal data captured during the recording of the event and the video testimonials.

Data subjects and categories of personal data

Externals

Social	
Social Media Account	
Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Contact Details	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	
European Patent Register Data	
Data provided by the data subjects	
Professional Experience & Affiliations	

CV	
Correspondence	
Personal information provided voluntarily	
Employment Information	
Company Entity	Job Title Role
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Personal Identification	
Age	Full Name
Gender	Nationality
Picture	
Education & Skills	
Educational Degrees	Languages

Employees

Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Working email address	
Building area and site	
Building area and site	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	
Correspondence	
Personal information provided voluntarily	
Employment Information	
Department name and/or number	
Browsing Information	

Browsing Time	Cookie Information
IP Address	
Personal Identification	
First Name	Gender
Surname	

Recipient of the personal data

Recipients of the data - On a need-to-know basis, the EPO staff working in PD Communication, Vice-President's office, Diversity&Inclusion team, and the Chief Sustainability Officer
- The external provider Regiepapst when creating the landing page and managing the vMix tool used for the streaming of the event.
- The EPO employees and the general public through the landing page created by Regiepapst for the event and its live streaming through the EPO's social media accounts.
- Facebook, YouTube, LinkedIn and Instragram social media platforms.
- Slido whenever non-anonymous questions or comments are sent by the data subjects thro

Purpose of sharing - On a need-to-know basis, the EPO staff working in PD Communication, Vice-President's office, Diversity&Inclusion team, and the Chief Sustainability Officer for the selection of the panellists and video testimonials, the preparation of the script for the panel discussion, and the management of the Slido tool during the event.
- The external provider Regiepapst has access to personal data for maintenance and technical purposes when using the vMix tool during the event
- The general public has access to the data subject's personal data for the promotion of the activity carried out by the EPO on the International Women's day.
- Facebook, YouTube, LinkedIn and Instragram social media platforms are used to promote and stream the event, so that the Office reaches the widest possible audience.
- Slido whenever non-anonymous questions or comments are sent by the data subjects through it.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 159

Name Access Control and Card Management Systems - DG4 -PD44 - General Administration

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 44 - General Administration

Entity Name - Processor (Entities)

External processors

Security Services Contractor at the EPO site of Berlin

External processors	
Name Security Services Contractor at the EPO site of Berlin	

Description of the processing

Description The Card Management System is used to register the data subjects and to provide them with access badges to be used to enter the EPO premises in a controlled way.
Prior to production of the access cards, the identity of the recipients and the authenticity of the document presented is verified by means of identity document scanners.
During the process the data in the document and the chip (if available) is verified and immediately discarded once the result is presented. There is no data recorded.
The access control system (AEOS) is a software application that is used Office-wide to manage access within the different EPO sites and is managed by the Facility Management Directorate.
The AEOS application registers EPO staff, contractors, service providers and visitors via web server application installed under EPO servers.
The application is connected to the card management system (CMS Nexus Prime application which is fed by SAP FIPS), from which

it receives the information. In addition to the data fields exported by the CMS, AEOS stores also the access profiles of each data subject and the access logs of the readers where the users presented their access badge, regardless to whether access is granted or not.
All data received by the access control system comes from FIPS via the card management system.
The access profiles are used to grant or deny access to individual access points (card readers) in the EPO buildings.

VISITOR ACCESS
The system is also used for registering and granting access to visitors in the sites where access control readers are installed. In those sites the external security provider registers visitors at the reception of each building using the AEOS application. The data is then stored in a central access control database and used to distribute the right badge that each visitor is requested to wear during the time of their visit. The data registered from visitors is obtained from their identity document and includes some of the details mentioned in the identity document presented by the visitor including name, family name, date of birth and/or identity document number. In addition there are some other details including visitor badge number, contact person and company also added to AEOS.
For EPO's employees family members (FIPS registered partners and dependent children from EPO staff above the age of 16), personal data are processed in order to provide them a family badge to access the EPO sport facilities and semi-public areas if so requested via MyFIPS interface by the sponsoring staff member. The badge will contain their picture, full name and ref. to the EPO staff member that is linked to the family member. Additionally the EPO Fitness Club Manager will use it to register fitness club members and give them access to the fitness rooms. There is an automated e-mail sent to individual fitness club members when their membership to the club is due to expire.
All data categories contained in a travel document (passport or national identity card) are processed but not stored. They are only processed during the identity verification done by means of identity document scanners being discarded once the result is presented.

CO2 EMMISSIONS
In order to calculate the impact that the usage of private own staff vehicles have on CO2 emissions, the access control database from the AEOS application, is queried by an algorithm (via SQL script), programmed by the company NSecure, that extracts the amount of vehicles belonging to permanent employees that access the parking facilities in Munich and The Hague.
In Munich, this is done by analysing the number of permanent employees presenting their badge in the access control readers that provide access to the parking lots in their premises.
In The Hague site this is done by querying the same data group but extracted from the Automatic Number Plate Recognition system

Purpose of Processing The card management system application is used to: 1. Manage access badges to provide access to buildings to EPO staff, family members, Council members, patent attorneys, contractors, EPO pensioners, service providers and visitors; 2. Verify that the visitors are not in the House Ban list (See Genehmigungsschreiben of 288/16) and as such allowed to enter the EPO Premises before a visitor badge is assigned to them; Verify the identity of the persons getting an EPO access badge by means of automated identity scanners, which at the same time also verify the authenticity of the identity document scanned. In the access control system personal data is processed for the purpose of managing access to the different EPO buildings and parking facilities in an efficient and effective way. The access control system is also used to monitor compliance with the existing provisions (House Rules and Security Circulars) as well as to: 1.- Provide access to EPO staff, visitors and contractors, including service providers, to EPO buildings; 2.- Register the access logs to areas where access has been granted to users; 3.- Register in an automated way (upon arrival of the vehicle to the entrance of the parking) the vehicle number plate of staff, contractors and visitors vehicles having access to EPO premises in order to: a) Monitor parking usage and limit the intervention of administrative staff for the registration of long term parking requests. b) Automate the way staff is informed whenever they violate the parking rules leaving their vehicles for longer terms than permitted (e.g. sending automated e-mails to staff not respecting the parking rules). c) Manage in a more efficient way the available parking facilities (one vehicle per staff member). To achieve No. 3, the number plates of the vehicles approaching the entrance of the parking are registered and linked to their access badge, this is done in order to identify the owner of the vehicle and to be able to monitor parking usage (one vehicle per person, one day maximum allowed parking time). 4.- Trigger alarms via Security Management System including door too long open alarms, forced opening of an entrance door or perimeter door and non-authorised badge used in an entrance.

(ANPR) cameras that are located at the entrance of the parking lot of that site.
The results of both data sets are an anonymous statistical data set that contains only figures related to each site, serving as base for the analysis of the CO2 impact that The Office envisages to collect and analyse. The information is provided via e-mail Excel attachment sent by the access control software AEOS using the SMTP email server of the EPO as runway.

Groups or persons concerned:
 EPO employees
 EPO employees family members (above the age of sixteen)
 EPO pensioners
 Visitors
 Service providers
 Canteen users
 External persons
 DPMA Berlin Office staff
 Patent Attorneys
 Council members.

Data Retention ACCESS CONTROL SYSTEM
Access logs older than 12 months will be overwritten by an automated routine programmed in the software.
Visitor data will only be kept for 28 days in line with the video surveillance records and for security purposes. This will allow physical security to proceed supporting investigations involving visitors access if criminal offences are reported.
In the event of a formal appeal/litigation, all data held at the time of the formal appeal/litigation shall be retained until the completion of its process.

CARD MANAGEMENT SYSTEM
Data coming from FIPS will be stored and deleted following the retention times established by FIPS (an employee or contractor user data will be deleted upon deletion in FIPS).
For groups such as the Administrative Council or Patent Attorneys added manually by the so-called data manager, this one will perform, at least once per year or whenever a change is reported to them, a sanity check. During this check the data manager will verify if the data is still valid and correct, performing any necessary changes and/or deletions to keep the data up to date.
In the event of a formal appeal/litigation, all data held at the time of the formal appeal/litigation shall be retained until the completion of its process.

Data subjects and categories of personal data

Employees

Sensory and Electronic Information	
Time stamps from their access to the buildings	
Contact Information	

Phone Numbers	Working email address
Employment Information	
Benefits and Entitlements Data	Business Unit Division
End Date	EPO access badge number
Language preference (of communication)	Office Location
Start Date	
Personal Identification	
Full Name	Gender
Unknown	
EPO badge validity	Price list for discounts
Government Identifiers	
Passport Number	

Externals

Sensory and Electronic Information	
Time stamps from their access to the buildings	
Employment Information	
EPO access badge number	
Unknown	
EPO badge validity	
Personal Identification	
Date of Birth	Full Name
Government Identifiers	
National Identity Card Details	Passport Number

Contractors

Sensory and Electronic Information	
Time stamps from their access to the buildings	
Contact Information	
Phone Numbers	Working email address

Employment Information	
End Date	EPO access badge number
Language preference (of communication)	Office Location
Start Date	
Personal Identification	
Full Name	Gender
Unknown	
EPO badge validity	Price list for discounts
Government Identifiers	
Passport Number	

Former Employees

Sensory and Electronic Information	
Time stamps from their access to the buildings	
Contact Information	
Personal Email	
Employment Information	
End Date	EPO access badge number
Personnel Number	
Personal Identification	
Full Name	
Unknown	
EPO badge validity	
Government Identifiers	
National Identification Number	Passport Number

Recipient of the personal data

Recipients of the data Personal data registered is accessible to those organisational units working in security or reception services during the retention period established and for the performance of their duties (monitoring and managing security and safety processes, responding to alarms).
The EPO Technical Department experts, PD 4.4 Advisory Services for the service and updates of the application, and technicians and the external maintenance company technicians have access to the application and its hardware for the performance of the maintenance of those ones.

The data is only used internally by FM security section staff and its external security contractor staff. If other recipients (e.g. Ethics and Compliance, Police, Safety Expert) request access to the personal data this will be individually asked to the Delegated Controller consulting DPO for advice.

Purpose of sharing N/A

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures
ACCESS CONTROL SYSTEM Access to the data stored in the access control logs is limited to the administrators of the application. The data will only be accessed upon request and with the permission from the Controller after having obtained favourable advise from the DPO, except in extreme urgency cases in which DPO will be informed. Other users with access to the data such as the external security contractor will only have access to the data stored for the purposes of registering access control, visitor management and number plate registration (parking management). Access to the application and the data stored on it is limited to those with a need to know. Administrators from EPO Security have access to stored log files to monitor compliance and the external security contractor has limited access to operate the application. Access to the application requires the authentication via BIT tools (password/active directory) plus an additional password for the application. All personal data is stored in secure IT applications according to the security standards of EPO. These include: User authentication: All workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): Separation into administrative and user roles, users have minimum privileges, reduction of overall

administrative roles to a minimum; Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices; Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; Security incidence response: 24/7 monitoring for incidents, on-call security expert. CARD MANAGEMENT SYSTEM Access to the data stored in the access control logs is limited to the administrators of the application. The data will only be accessed upon request and with the permission from the Controller after having obtained favourable advise from the DPO, except in extreme urgency cases in which DPO will be informed. Other users with access to the data such as the external security contractor will only have access to the data stored for the purposes of registering access to the EPO premises. Access to the application and the data stored on it is limited to those with a need to know. Administrators from EPO Security have access to stored log files to monitor compliance and the external security contractor has limited access to operate the application. Access to the application requires the authentication via BIT tools (password/active directory) plus an additional password for the application. All personal data is stored in secure IT applications according to the security standards of EPO. These include: User authentication: All workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): Separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices; Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; Security incidence response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 161

Name Consultations and assessments of the capacity to work of staff by the EPO Occupational Health Services

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 423 - HR Essential Services

Entity Name - Processor (Entities) DG4 - 422 - HR Customer Engagement, DG4 - 46 - CIO / BIT

External processors

SAP

External processors	
Name SAP	

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description This record refers to the consultations with staff and the assessments of their capacity to work by the EPO Occupational Health Services (OHS).

The staff of the EPO OHS consists of medical, para-medical staff and administrative staff.
The EPO OHS process personal and medical data in order to support the health and wellbeing of staff, their reintegration to work after illness or accident and to provide medical opinions and measures to be taken (e.g adaptation of working hours) to other HR departments according to the

EPO Service Regulations.
They provide medical assessments in the following cases where staff members may be affected by illness or suffer from an accident:
a. Consultations
b. Medical examination in case of Extended Sick Leave or Incapacity
c. Duty of care medical examination
d. Verify sick leave
e. Validate absences from the place of employment during the sick leave

a. Consultations
Staff suffering from a medical condition can contact the Occupational Health Services to have a consultation.
Our medical and para-medical staff give general advice on health matters and support staff with several possibilities such as adaptation of the workplace, working time and duties.
Staff on sick-leave is contacted after 10 working days of sick leave and invited for a mandatory examination after 30 days of cumulated sick leave days.
BIT provide the Occupational Health Services (OHS) with the sick leave statistics.
Consultations take place in person or via MS Teams (video)call.
Adaptation of working conditions are communicated to the staff member, the line manager and HR for registration.
Relevant legal provisions: Art. 26b, Art. 26c, Art. 1A(1) Circ. No. 367

b. Medical examination in case of staff in Extended Sick Leave or Incapacity (i.e. staff who have cumulated more than 125/250 sick leave (SL) days within a period of 18/36 months)
BIT provide the OHS with sick leave statistics containing the names of the staff members who have accumulated more than 30 SL days in 1 year, 125 SL days in 18 months and 250 SL days in 36 months.
Information about recommended adjustments of working hours and conditions are provided to staff member, line manager, HR Interlocutors.
Relevant legal provisions: Art 62.a SR - Sick leave, Art 62.b SR - Incapacity,
Circ. 367 - Absences for health reasons, Title VI ServRegs (Medical opinions)

c. Duty of care medical examination in the interest of the Office and of staff that are or seem to be affected by a medical condition (in this case the EPO medical staff have to assess their capacity to work and issue the suitable reintegration plan)
This examination can be asked by the line manager (LM), the HR Business Partner (HRBP) and the HR director. The medical opinion issue by the EPO medical staff is shared with the requesters , the staff member, the HR Interlocutors. The EPO medical services express their opinion on the capacity to work of the employee, provide a reintegration plan and/or workplace adjustments.
Relevant legal provisions: Art 26(2) SR - Medical examination ordered by the President, Title VI ServRegs (Medical opinions)

Purpose of Processing Processing of medical data is necessary to provide medical opinions on the capacity to work when required by internal regulations., Processing of medical data is necessary to manage the sick leaves by providing professional support throughout the process of reintegration into work, Processing of medical data is necessary to promote and ensure the health, safety and wellbeing of the employees via the consultations between staff and the OHS staff

d. Verify sick leave
The sick leave verification can be requested by the line manager and/or the HR Business Partner and is approved by the HR Director. It is carried out at Office premises by EPO medical staff who provide an assessment to the HR Director on the capacity to work of the staff member without any further medical information. Staff member, line manager and HR business partner are informed of the results of the verification.
Relevant legal provisions: Art 62a.(6) - Sick leave, Circ. 367 art. 1B - Sick leave verification, Art. 91 ServRegs

e. Validate absences from the place of employment during the sick leave
To spend sick leave in a place other that their place of employment, the employees have to send a request to the HR Director who will grant it. HR Director may request the advice of the OHS.
The HR Director's decision is sent to the requester, their LM and the HRPB.
Relevant legal provisions: Art 62a (5) SR - Sick leave, Circ. 367 art. 1C

In all the case mentioned above:
•There is no exchange of medical information between the medical experts of the OHS and the management, the HRBP and the HR Interlocutors.
•Any medical information (e.g. date of the consultation, medical notes, medical reports) is stored in the EPO medical database (Cority) and only a limited number of medical, paramedical and administrative staff have access to the medical database on a need-to-know basis.

Data subjects are:
•Employees
•Treating physicians of the employee

In all the above mentioned procedures, the following categories of personal data may be processed:
Surname, forename, gender, personnel number, date and place of birth, nationality, civil status, languages, postal addresses, e-mail address, private/work telephone numbers, room number, name of treating physician, job profile, type of contract, line manager name, type and duration of absences from work, date/time of medical consultations, sickness statistics, sick leave certificates, medical opinions (always issued without medical data), location/period/contact data for spending sick leave away from the place of employment, capacity to work and work place adjustments (in particular in the framework of a reintegration procedure).

In all the above mentioned procedures, the following special categories of personal data may be processed.
Medical data: personal medical history, medical reports provided by the staff member, medical reports provided by EPO specialists after a consultation with the employee, medical notes recorded after a consultation, medical certificates, diagnoses.

Data Retention Cority is used since 2006 as main medical database. As of 2016, data are stored only electronically in the EPO medical data base (Cority).
Currently, the data is kept in the electronic database permanently due to technical constraints.
However, by 2023 the following period should be implemented for all the above procedures:
10 years as of end of service.
The retention periods apply unless a litigation is pending or the case is related to asbestos exposure or similar. In case of pending litigation, the retention period will be suspended until all means of redress have been exhausted or the decision has become final. In cases related to asbestos exposure or similar, retention will be decided case by case.

All data stored in the Outlook common boxes and calendars of the OHS older than 5 years is deleted.

Data stored in SAP-FIPS are currently stored permanently.

In principle all data are stored only electronically. However, there are still old medical paper files stored in secured locked rooms only accessible to authorized staff that should be deleted by 202.

Data subjects and categories of personal data

Employees

General	
Personal Information in SAP	Sensitive Personal Data in SAP
Special Categories of Data in SAP	
Ticketing	
Ticket related data	
Health Data	
Health Data	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Personal Email
Phone Numbers	Working email address
Correspondence	
Personal information provided voluntarily	
Employment Information	

Business Unit Division	Contract Type
Department name and/or number	End Date and Reason for Termination
Hours of Work	Job Group
Job Title Role	Line Reporting Manager
Office Location	Personnel Number
Record of Absence/Time Tracking/Annual Leave	Room Number
Start Date	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Marital Status	Nationality
Education & Skills	
Languages	

Externals

Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers
Employment Information	
Job Title Role	

Recipient of the personal data

Recipients of the data Employee – Staff member has the right to access their medical file in accordance with the applicable Data Protection Rules.

The following recipients may have access to the categories of personal data (excluding any medical data) mentioned under points 1.2 and 1.17 on a need-to-know basis only:
• HR Interlocutors – in particular they are the ones that receive and process the sick leave certificates and share them on a need-to-know basis with the OHS. OHS may request copy of sick leave certificates of staff in long term sick leave in order to be promptly informed about extension of the sick leave period and therefore provide any

suitable further support.
• Line manager and HRBP – exchange of information with the EPO medical practitioner in charge of the reintegration case can be normally made in order to support the full reintegration to work of the employee. No medical information is exchanged with them. Line manager and HR Business Partner may request such a meeting.
• Line Manager may have access to the private telephone number of their team to stay in touch with them in case of long absences (especially in case of sick leaves).
• Safety experts – in the framework of inquiry, management of any accident or incident occurred at the workplace
• Ergonomics experts – they carry out work place visits/arrangements triggered by the employee or the OHS staff for a proper ergonomic setup of the work environment
• ServiceDesk – OHS or the ergonomics experts can contact ServiceDesk in order to request to provide a staff member with ergonomic devices not included in the standard supplies.
• Legal Services may have access to personal data for the prevention and management of grievances
• Directorate Ethics and Compliance (DEC) may have access to personal data in the framework of their investigative mandate
• SAP–Centre of Excellence department – a very limited number of staff of this department provides technical support for the maintenance of the medical database (Cority), in particular for system configuration purposes (i.e. creation, update and deletion of general system settings including language; screen layouts including the configuration of fields displayed on screens; look-up tables; business rules including field input checks; roles and profiles) and users management (i.e. creation and deletion of user accounts and the assignment of roles)
• National authorities – a) in very exceptional cases, when the employee has a very serious mental illness that prevents them from taking care of themselves and puts them and/or others at serious risk and any other remedy has been exhausted, the EPO Medical Services may involved the national social/security services to protect the health, rights and freedoms of staff and/or others; b) when the employee fails to inform their line manager of their absence from work and all attempts made by the line manager and/or the EPO Medical Services to contact them have been unsuccessful, the EPO Medical Services may disclose personal information to national public authorities (e.g. police) in the exercise of its duty of care and to protect the health of the staff members. (Article 5e DPR)

The following recipients may have access also to the medical data mentioned under point 1.2 and 1.17 on a need-to-know basis only:
• Treating physician of an employee – a) when the employee has given the appropriate authorisation for the exchange information between their treating physician and the EPO medical practitioner (according to Article 89(3) ServRegs), b) when an employee is affected by severe psychiatric and psychological problems and they could suffer harm from knowing the content of a

Purpose of sharing

medical report/file (e.g. in the case of a documented suicide risk), in this case the access is given through the doctor of the employee's choice (Article 8 of the Circ. No. 420 Implementing Article 25 of the DPR).
• Emergency physicians / staff of the emergency medical service - in cases where the OHS deem an emergency medical intervention to be necessary and are aware of information essential to the health of the data subject and the data subject is not in a physical/mental condition to provide such information personally (Article 5e DPR)
• SAP–Centre of Excellence department – only one employee of this department with the role of system configurator is allowed to have full access also to medical data. This is a necessary requirement to ensure the functionality and efficiency of the application.

The data are not used for any other purposes nor disclosed to any other recipient.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States, SAP - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, Link to the Matrix of the access rights (https://epocloud-my.sharepoint.com/personal/mrossi_epo_org/Documents/Data%20Protection/DP%20Register/HR%20customer%20engagement/Medical%20files/old/Matrix%20of%20Cority%20access%20rights.docx?web=1), For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by

encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., Once a year (in Q1) a roles review and logs security audit is carried out. The user manager in SAP–Centre of Excellence department sends to the chief physicians of the EPO OHS the list of users and their respective roles assigned to Cority. The chief physicians must verify and validate the list and roles. The logs security audit is done by the chief physicians directly, each one for the data they are responsible for., Medical reports are sent via email to the staff member after being encrypted or password protected in accordance with the Office’s recommendations (Outlook Migration to the Cloud- http://my.internal.epo.org/portal/private/epo/organisation/dg1/?WCM_GLOBAL_CONTEXT=/epo/intranet/organisation/dg1/vp1_org/announcements/2021/1612436889418_outlook_encripted_documents), Administrative staff of the EPO OHS, HR Interlocutors, HR Officers and the system configurator of the SAP-Centre of Excellence department are required to sign a confidentiality and data protection declaration, The access to the medical data base is strictly given only to authorised persons, namely • the EPO medical and para-medical staff, • the administrative staff of the medical services, • the System Configurator of the SAP–Centre of Excellence department, • the Emergency User - In urgent cases it is essential that an emergency user exists, in order to intervene in cases of severe malfunction of the system (such as failure of the system, total authorisation blockage or process deadlock). Therefore the emergency user needs the complete Cority access rights. The emergency user has full authorisation allowing the execution of all system and application functions without any authorisation restrictions The access rights allow the above mentioned staff to process and consult only the data for which they are responsible, When face-to-face consultations are not possible or the staff member prefers to have remote consultations, MSTeams is the application used in these cases. Staff is informed not to share messages or documents containing sensitive information during MSTeams (video)calls in accordance with the Office’s recommendations (Using Microsoft Cloud tools- http://my.internal.epo.org/portal/private/epo/work/news/?WCM_GLOBAL_CONTEXT=/epo/intranet/work/news/2020/1588753875455_using_cloud_based_tools).

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 164

Name Identity Management through AD and Azure AD

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description This record encompasses provisioning of user accounts and related user access rules and allocations through the use of Active Directory (AD) and Azure AD as the central repository of user identities.

Two scenarios for provisioning of user accounts are currently in place:
1. Internal (employees and contractors) users are defined in FIPS (master) which is synchronised with On Premise AD using Microsoft Identity Manager (MIM). Subsequently, the On Premise AD is synchronised with Azure AD using Azure AD Connect.

2. Users of national patent offices: the master is Single Access Portal, where users are created, updated and deleted, which is synchronised with On Premise AD using Microsoft Identity Manager (MIM). Subsequently, the On Premise AD is synchronised with Azure AD using Azure AD Connect.

User accounts are subsequently used for authentication and authorisation purposes.

Data Retention User data is kept until flagged inactive in the master (source) system (i.e. FIPS or Single Access Portal) and then kept in both On premise AD and Azure AD for additional 30 days.

At all times during the term of EPO's subscription, EPO has the ability to access, extract and delete the data stored in the applications in scope of this record. Microsoft will retain EPO data that remains stored in the applications in a limited function account for 90 days after expiration or termination of EPO's subscription so that EPO may extract the data.

After the 90-day retention period ends, Microsoft will disable EPO's account and delete the EPO Data and Personal Data within an additional 90 days, unless Microsoft is authorized under the agreement with EPO to retain such data.

For Personal Data in connection with the applications in scope of this record, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon EPO's request, unless authorized under the agreement with EPO to retain such data.

Purpose of Processing Provisioning of user accounts and related user access rules and allocations for authentication and authorisation purposes

Data subjects and categories of personal data

Contractors

Network/application Interaction Data	
Session details	Session metadata
Physical and/or Digital Identifiable Assets	

Digital Certificate	Mobile Device Name
Operating System Version	Workstation's Hostname (Physical or Virtual)
Contact Information	
Mobile Phone Number	Phone Numbers
Working email address	
Building area and site	
Building area and site	
Device Management Data	
Account ID	Azure Active Directory Device ID
Last Logon Time	Tenant ID
Windows ID for Windows Devices	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
IP Address	
Employment Information	
Active/Inactive Indicator	Business Unit Division
Company Entity	Department name and/or number
Job Title Role	Language preference (of communication)
Line Reporting Manager	Office Location
Personnel Number	Room Number
Personal Identification	
Digital signature	First Name
Gender	Surname
Picture	
User Account Information	
Account Age	Account Password

Membership Permissions	Ownership Permissions
Password Hash	User ID
System Logs	
Audit Logs (a.k.a. Audit Trail)	System-, Application-, Security-related Server Logs

Employees

Network/application Interaction Data	
Session details	Session metadata
Physical and/or Digital Identifiable Assets	
Digital Certificate	Mobile Device Name
Operating System Version	Videoconference Room/Equipment Identifier
Workstation's Hostname (Physical or Virtual)	
Contact Information	
Mobile Phone Number	Phone Numbers
Working email address	
Building area and site	
Building area and site	
Device Management Data	
Account ID	Azure Active Directory Device ID
Last Logon Time	Tenant ID
Windows ID for Windows Devices	
Browsing Information	
Browser type	Browsing Time
IP Address	
Employment Information	
Active/Inactive Indicator	Business Unit Division
Department name and/or number	Job Title Role
Language preference (of communication)	Line Reporting Manager

Office Location	Personnel Number
Room Number	
Personal Identification	
Digital signature	First Name
Gender	Surname
Picture	
User Account Information	
Account Age	Account Password
Membership Permissions	Ownership Permissions
Password Hash	User ID
System Logs	
Audit Logs (a.k.a. Audit Trail)	System-, Application-, Security-related Server Logs

Externals

Network/application Interaction Data	
Session details	Session metadata
Contact Information	
Country	Mobile Phone Number
Phone Numbers	Working email address
Employment Information	
Company Entity	
Browsing Information	
Browser type	Browsing Time
IP Address	
Personal Identification	
First Name	Surname
User Account Information	
Account Age	Account Number

Account Password	Membership Permissions
Ownership Permissions	Password Hash
System Logs	
Audit Logs (a.k.a. Audit Trail)	System-, Application-, Security-related Server Logs

Former Employees

Network/application Interaction Data	
Session details	Session metadata
Browsing Information	
Browser type	Browsing Time
IP Address	
Personal Identification	
First Name	Surname
User Account Information	
Account Age	Account Password
Membership Permissions	Password Hash
User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	System-, Application-, Security-related Server Logs

Recipient of the personal data

Recipients of the data Internal Recipients:

- All EPO staff / contractors
- EPO’s staff members from D4623 – IT Security
- Any application which is allowed to interrogate EPO AD/Azure AD to perform user authentication and authorization.

External Recipients:

- Microsoft

If other recipients request access to the personal data, this will be individually asked to the Delegated Controller consulting the DPO for advice.

Purpose of sharing Access to personal data is provided on a need to know basis, only to the necessary categories of personal data depending on the recipient.

Internal Recipients:
- All EPO staff: read access (directly via browser) e.g. via phone book or indirectly via APIs to other Microsoft applications (e.g. Outlook, MS Teams, etc.) to personal data of other EPO staff

- EPO’s staff members from D4623 – IT Security: AD & Azure AD administrators

- AD/Azure AD personal data are accessed by EPO applications for user authentication/authorization purposes.

External Recipients:
- Microsoft is a recipient for support, maintenance and security services.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Protection against malware, login to Azure Active Directory, error analysis, load balancing, diagnostics data and processing for Microsoft’s business operations

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures Azure Active Directory is certified according to several security standards (e.g. SOC 1 Type II, SOC 2 Type II), For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., For Identity Management systems hosted at EPO premises, the following security measures are in place: All personal data related to Identity management are stored in secure IAM applications according to the security standards of EPO. These include: • User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; • Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; • AV on all devices • Physical protection: EPO access controls, additional access controls to datacentre, • Transmission and input controls: audit logging, systems and network monitoring): security monitoring with Splunk; • Security incidence response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

Data Protection Statement link internet Data Protection Statement will be prepared and published when the record is approved by the DPO.

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 165

Name Microsoft Defender for Endpoint

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description Microsoft Defender for Endpoint (MDE) is a platform which collects security relevant event data from onboarded endpoints (Windows workstations and Windows servers) and transmits it to an EPO MDE dedicated and segregated cloud tenant for processing and alerting in an automated manner.

BIT PD 4.6 collects MDE security alert-related data from the MDE cloud tenant and stores this on premise in Splunk in an automated manner.

The further processing of personal data within Splunk is described in the dedicated Splunk record.

Purpose of Processing The purpose of the processing is for the Information Security Team to be able to: - prevent security incidents affecting the EPO network and data, such as malware infections - detect and alert to compromises or malicious activity on endpoints in the EPO's infrastructure - investigate and remediate security incidents in the EPO's infrastructure

Data Retention Personal data are stored in logically different places with the following retention rules:
- data stays in a temporary cache area in the endpoint itself, for max 3 days.
- MDE Security alert/incident related data is retained on premise in Splunk for 12 months
- data stay in MDE cloud environment for 180 days, after which it is deleted from MDE cloud tenant
The retention period for the transferred data in the Microsoft Defender for Endpoint Central Unit is no longer than 180 days; after 180 days, data is erased.

Data subjects and categories of personal data

Contractors

Network/application Interaction Data	
Session details	Session metadata
Physical and/or Digital Identifiable Assets	
Operating System Version	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Contact Information	
Phone Numbers	Working email address
Device Management Data	
Azure Active Directory Device ID	
Employment Information	
Department name and/or number	Job Title Role
Browsing Information	
Browser type	Browsing Date and Time
Browsing Time	Category
IP Address	Network Interaction History
URL	Website History
Personal Identification	
First Name	Surname
User Account Information	
Account Number	User ID

System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Ports	Registry data
Running Processes	System-, Application-, Security-related Server Logs

Employees

Network/application Interaction Data	
Session details	Session metadata
Physical and/or Digital Identifiable Assets	
Operating System Version	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Contact Information	
Phone Numbers	Working email address
Device Management Data	
Azure Active Directory Device ID	
Employment Information	
Department name and/or number	Job Title Role
Browsing Information	
Browser type	Browsing Date and Time
Browsing Time	Category
IP Address	Network Interaction History
URL	Website History
Personal Identification	
First Name	Surname
User Account Information	
Account Number	User ID
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Ports	Registry data

Running Processes	System-, Application-, Security-related Server Logs

Externals

Network/application Interaction Data	
Session metadata	
Browsing Information	
Browsing Time	IP Address

Recipient of the personal data

Recipients of the data Recipients of personal data (accessing the data via MDE cloud tenant console on strictly need-to-know basis) are:
- named individuals in EPO 4623 Information Security department
- named individuals having the role Microsoft O365 Global Administrator or the role Microsoft O365 Reader.

Recipients of MDE personal data (stored on EPO premises), on strictly need-to-know basis are:
- members of Dept. 4623 Information Security and Contractors who support Splunk infrastructure and application.

If people or entities other than those mentioned above would request access to MDE personal data, this will be individually asked to the Delegated Controller DP4.6 consulting DPO for advice.

Purpose of sharing Personal data are shared with EPO 4623 Information Security department with the purpose to: - prevent security incidents affecting the EPO network and data, such as malware infections - detect and alert to compromises or malicious activity on endpoints in the EPO's infrastructure - investigate and remediate security incidents in the EPO's infrastructure.

Personal data are shared to named, authorised individuals who have been assigned with the role O365 Global Administrator or O365 Global Reader, in order to let them perform O365 administrative tasks and activities.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Data could be transferred potentially for: protection against malware, login to Azure Active Directory, error analysis, load balancing, diagnostics data, connected experiences, and processing for Microsoft's business operations, Pseudo-anonymised ("Scrubbed") data is sent to central scale unit for threat analytics in the USA.

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., EPO uses role-based access to control access to the MDE console and data. All MDE activities done by any staff with legitimate access are logged and audit trails of such activities is kept.

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 167

Name Medical certificates/consultancy registration process

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 422 - HR Customer Engagement

Entity Name - Processor (Entities) DG4 - 423 - HR Essential Services, DG4 - 46 - CIO / BIT

External processors

SAP

External processors	
Name SAP	

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description All staff members are required to be certified sick by a medical practitioner or by OHS (Occupational Health Services-D) as from the fourth (working) day of sick leave accrued in any calendar year as lined out in Art. 62a ServRegs and Circ. 367.

The medical certificate should state:

Your name and date of birth
The date of issue of the certificate
The name and signature of the doctor
The start date and estimated end date of the absence for health reasons

No diagnosis is to be included.

Staff is informed that no medical details are to be included. If they choose to send it anyway (e.g. if they send the version of the medical certificate including the diagnosis code, which they should not, because there is a specific version for employers), it is ignored by HR interlocutors (referred to as HRIs in the following text) and deleted after the retention period.

The procedure for submitting the certificate is as follows:

Scans or photographs of the medical certificate shall be sent by email as an attachment. It will be handled by the HRIs. The personal EPO email address is to be included in the subject line of the email to allow efficient processing.

If staff send the email to the common box of HR Services, a ticket is created automatically in the HR ticketing system. From there, it is re-directed to the email inbox of the HRIs.

If staff is unable to send the certificate by e-mail then a copy (not the original) or the contact details of the treating doctor may exceptionally be sent by normal post to the HRIs. Those will scan the document on behalf of the employee.
Staff must keep the original of the medical certificates for four years.

If the treating doctor refuses as a point of policy to issue a certificate then staff shall send the name, address and phone number of the doctor to medicalcertificate@epo.org. The HRIs will never contact the doctor to ask for any details, however, the information about the treating doctor may be sent to OHS on request and they may exceptionally contact the treating doctor.

The HRIs register the certified period as "certified sick leave medical certificate" in the system via FIPS in case a medical certificate was received or "certified sick leave doctor consulted" in case the name and address of the treating doctor was received or "certified sick leave OHP (Occupational Health Physician) consulted" if a notification from OHS was received.
Only the HRIs have access to the medical certificate inbox. OHS may request copy of sick leave certificates of staff in long term sick leave in order to be promptly informed about the extension of the sick leave period and therefore provide any suitable further support. Certificates are never forwarded to any other party (such as line managers or HRBPs).

Staff members may alternatively consult OHS in case of sickness. In this case OHS will be sending a notification to the HRIs via the medicalcertificate@epo.org email address for registration of sick leave certification or reduced working time.

When returning to work, employees must notify the administration via the return from sick leave notification in myFIPS, the link being sent to them

Purpose of Processing Ensure compliance with the sick leave certificate regulations (Art. 62a ServRegs, Circ. 367)

via email.

The emails received are kept in a "recorded" subfolder of the email inbox. The full content of the folder is deleted at the end of the retention period including all attachments. Only the records in SAP remain (e.g. certified sick leave period with start and end date). For statistics purposes the amount of emails received per year is kept in an excel table. The amount refers purely to the number of emails received, fully anonymized (no data at all).

The documents received in paper are stored in a locked cupboard in one of the HRI's offices and destroyed after the retention period by an HRI by shredding or putting them in boxes dedicated to destruction of confidential documents in the office.

HRIs are bound by confidentiality and have also signed an ad hoc declaration of confidentiality.

Data Retention All paper certificates are kept for 4 years and then destroyed.
All certificates sent via email are deleted after 4 years.
Currently the entries about the certified periods remain in SAP-FIPS permanently.
For the retention period of data stored in the HR ticketing system, please refer to the relevant data protection statement

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	
Personal Identification	
Full Name	

Employees

Ticketing	
Ticket related data	
Contact Information	
Country	Home Address
Personal Identification	
Date of Birth	First Name
Full Name	Gender
Surname	

Recipient of the personal data

Recipients of the data The HRI team have access for the administration of the sick leave certificates of the employees.
OHS may request copy of sick leave certificates of staff in long term sick leave in order to be promptly informed about extension of the sick leave period and therefore provide any suitable further support. r for follow-up of extended sick leave or Incapacity cases.
Line manager may be informed about the certified period of absence but they do not get copy of the certificates.
BIT may provide technical support

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States, SAP - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 169

Name Evaluation of coaching and/or other development initiatives

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 421 - Talent Management

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description Personal data is processed to evaluate the effectiveness of the coaching and other development initiatives.

In order to evaluate said effectiveness the following tools are used:
1. Microsoft Forms to run polls and surveys
2.Diagnostic tools provided by the data processor SHL (i.e. the Occupational Personality Questionnaire, the Managerial Scenarios test and the 360 feedback review).

1. Surveys/polls

In principle, the surveys and polls are anonymous, however the data subjects are invited to respond surveys or live polls at different points in time during and/or after the development initiative.

The analysis of the aggregated and anonymised answers to the polls/surveys is shared with EPO senior management to provide insights into the effectiveness of coaching and other development initiatives.

2. Diagnostic tools provided by the data processor

These are the steps that the data processor performs in order to process the data related to the diagnostic tools:

- They extract from the online assessment platform the list of names, email addresses and related tests/questionnaires' results saved in the system within the period of time provided by EPO.
- Afterwards only the data of EPO employees identified in writing by the EPO are analysed.
- The full list of all employees is without undue delay deleted after identification of the respective candidates
- The list of EPO employees identified in writing by the EPO is anonymised or deleted upon the written request of the EPO Talent Academy
- They consolidate the information and provide the EPO Talent Academy with the analysis of the aggregated and anonymised results.

The analysis of the aggregated and anonymised results is shared with EPO senior management to provide insights into the effectiveness of coaching.

Data Retention 1. Surveys/Polls

Data will be kept only for the time needed to achieve the purposes for which it is processed. Then, data will be deleted after 5 years as from the end of the survey/poll. The aggregated and anonymised reports will be kept indefinetly.

2. Diagnostic tools provided by the data processor

The personal data are used only to extract the assessment scores and will then be without undue delay deleted by the data processor.

Purpose of Processing Measurement of the effectiveness of the coaching programme and/or other development initiatives.

Data subjects and categories of personal data

Employees

Contact Information	
Personal Email	
Learning managements metrics	
Diagnostic tools’ results	Ratings
Personal Identification	
Full Name	

Externals

Learning managements metrics	
Ratings	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data Personal data will only be shared on a strictly need to know basis - personal data are only processed by the EPO Talent Academy and the data processor.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 175

Name Employee Assistance Programme (EAP)

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 422 - HR Customer Engagement

Entity Name - Processor (Entities)

External processors

LifeWorks

External processors	
Name LifeWorks, LifeWorks	

Description of the processing

Description Staff member or dependent may contact the EAP Care Access Centre for confidential short-term counselling to solve personal or work-related problems, pressures and stress situations.

In particular, assistance is provided for:
• Coping with isolation and loneliness
• Adapting across cultures
• Identifying and coping with culture shock
• Addressing the personal impact of the relocation
• Dealing with stress, anxiety, and depression
• Addressing alcohol and drug misuse
• Resolving marital and relationship difficulties
• Finding solutions for work-related issues
• Offering advice and referrals for work-life issues such as family support / parenting / elder care
• Accessing crisis and trauma support
• Address legal or financial issues
• Working towards life goals
• Strengthening relationships
• Improving communication

The Procedure can be described as follows.

- The first contact is made by phone .
- The staff members/dependents have to provide the name of the EPO in order to identify the employer offering this service.
- They are free to decide to remain anonymous by using a pseudonym.
- Email address and / or phone number are needed by the provider as contact data.
- Other personal data and information might be asked according to the kind of support that is provided. These additional personal data are always taken for the purpose of providing the specific support the person requests.
- After a preliminary case assessment, the EAP Care Access Centre identifies a specialist with whom the staff member/dependent can have approximately 6 support sessions over the telephone, online or in person.
- If the staff members/dependents need more specialised or long-term support, the service provider will help them select an appropriate specialist or service.
- Once a case is closed, the staff member/dependent is asked by the provider to evaluate the service via an anonymous survey.
-Quarterly and annually the D4225 Wellbeing and Engagement receive aggregated data reports by the service provider.
- In addition the EAP offers an online platform, called LifeWorks, that can be accessed via an app or PC. Credentials to access this platform are EPO bound, not individual.
- The platform provides information about health and wellbeing and offers the possibility to contact the EAP care access centre.

Information relating to participation in the EAP is strictly confidential. No information is shared with anyone without informed, voluntary and written consent. Only in order to protect the vital interest of the staff/dependent or third parties, the external service provider can, and has to, inform the national authorities and disclose personal data.

For the vast majority the personal data processed by Allianz and LifeWorks, the EPO is not the controller. In principle, Allianz and LifeWorks are the controller of the personal data provided directly by the users of the Services.

A DPA (Data Processing Agreement) should be signed between the EPO and LifeWorks Ltd. by 2022 only with regard to the processing of personal data carried out on the platform provided by LifeWorks.

Data Retention This information is missing pending the finalization of the DPA (Data Processing Agreement) that should be concluded between the EPO and LifeWorks Ltd.by 2022. The DPA should relates to the processing of personal data carried out on the platform provided by Lifeworks.

Purpose of Processing - Providing staff members and their dependants with free access to psychosocial support and counselling if there is a need to help reconcile work and home life. - Making sure the right support is given and the needs are addressed accordingly by receiving the relevant and correct data from the person, Access to the online platform

Data subjects and categories of personal data

Employees

Employees

Health Data	
Health Data	
Contact Information	
Home Address	Personal Email
Phone Numbers	
Employment Information	
Company Entity	

Externals

Health Data	
Health Data	
Contact Information	
Home Address	Personal Email
Phone Numbers	
Employment Information	
Company Entity	

Recipient of the personal data

Recipients of the data Within EPO
Only aggregated data or the anonymised surveys are shared with D4.2.2, PD4.2, VP4, President, COHSEC.

Outside the EPO
LifeWorks known before as Morneau Shepell - (the Sub-Processor) is the party that deals with all the processing of personal data and it is the only party that has access to raw personal data.

Allianz Partners - (the Data Processor) only receives the data EPO receives i.e. results of aggregated anonymised reports of service satisfaction and the "Utilisation Report".

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) LifeWorks - United Kingdom

Reasons for the transfer The external processor is based in the UK

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 177

Name Physiotherapy service

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 423 - HR Essential Services

Entity Name - Processor (Entities)

External processors

B&R Health Management

External processors	
Name B&R Health Management	

Description of the processing

Description The service:
- The Physiotherapy Service is provided exclusively by external service providers, namely High-Five in Munich and B&R Health Management in Netherlands.
- The service providers and all the sub-processors involved for the purpose of physiotherapy services are located in EEA and therefore bound by the EU data protection regulation.
-Physiotherapy services are offered to all EPO staff-members

The procedure:
- When a staff member is interested, the staff member contacts the Physiotherapist providers directly by finding on the intranet the contact details of the Physiotherapists and also information about the tools they need to use to book an appointment.
- Appointments can scheduled by phone, e-mail, direct contact or via the online booking tool.
- On the day of the appointment, the staff member will be invited to share with the Physiotherapist the necessary personal and medical data needed for the service.
- All the personal data are shared by the staff-member that requests the service.
- All these data are stored as medical files in the databases the providers use.

Data storage and retention:

- The external service providers use their own applications only not the ones of the Office so EPO has no access to these tools.
- All IT applications used by the service providers for the provision of the service (e.g. scheduling, invoicing, maintaining the patient history for the provision of the physiotherapy services, complying with national regulations) are stored in data centres located in the EEA.
- Paper files containing medical data (e.g. doctor's prescription, medical notes) are stored in locked cupboards in the physiotherapy rooms and the keys are available only to the physiotherapists.
- Usually what the physiotherapists put on paper is only their personal schedules. The medical data is stored in the online tools the service providers use so medical data are not stored on paper.

The external service providers provide a yearly anonymous report that shows the most common injuries and what are the most common reasons the staff members contact the physiotherapists.

The EPO does not receive any personal or medical information on its staff from the external service provider.

Data Retention Payment information and medical files are retained according to the applicable national regulations. During this retention period data will not be anonymised nor pseudonymised.
After this retention time the data will be deleted.

Purpose of Processing Provide anonymized report to D423, Offer preventive physiotherapy advice as well as physiotherapy treatment for the staff members. Make sure the service is provided effectively and it is easy to reach.

Data subjects and categories of personal data

Employees

Health Data	
Health Data	
Contact Information	
Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Working email address
Building area and site	
Building area and site	
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Financial	
Bank Account Information	
Employment Information	
Weight	
Personal Identification	
Age	Date of Birth
Full Name	Gender
Height	Nationality

Externals

Contact Information	
Contact Details	

Recipient of the personal data

Recipients of the data External providers and their sub-processors for the administration and management of the services (e.g. scheduling, invoicing, maintaining the patient history for the provision of the physiotherapy services, complying with national regulations)

D423 receives only anonymized aggregated data for analysis purposes.

The data are not used for any other purposes nor disclosed to any other recipient.

Purpose of sharing

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 178

Name Registration of Munich staff's children in crèches subsidised by the Office

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 423 - HR Essential Services

Entity Name - Processor (Entities)

External processors

AWO-Isar

External processors	
Name AWO-Isar	

Description of the processing

Description In-house crèche
Personal data are processed in order for Munich staff to apply for a place in an in-house crèche via a dedicated online registration tool accessible from the EPO intranet.

Once the EPO staff members submits their application, they are automatically registered in the registration tool managed by D4233 under the status "inscribed" and an automatic 'receipt of request' confirmation is sent via Outlook to the staff member.
D4233 Expatriation and Social Services revises the request, i.e., confirms directly with the in-house crèche whether there is a vacancy.

In case there are no vacancies, no communication is sent to the staff member. When a place becomes available however, D4233 sends an offer by e-mail to the staff member concerned and includes the crèche in Cc. The EPO does not transmit personal data included by the staff member on the dedicated tool to the crèche – only

name and surname of the parent(s) and child and birthday of the child are included in the e-mail. The staff member is instructed in said e-mail to contact the crèche directly in order to proceed with the enrolment of their child.

In case the staff member accepts the offer, they are to inform D4233 who, upon such confirmation, will change the status in the registration tool from “inscribed” to “under offer”.

In case the staff member refuses the offer, they are to inform D4233. The status in the registration tool will be changed by D4233 from “under offer” to “cancel”.

In case the staff members contracts with the crèche, the staff member and/or the crèche informs D4233 when they accept the place. The status change is then changed by D4233 in the registration tool from “under offer” to “placed”.

In case of terminations, the crèche sends a termination confirmation to the staff members with D4233 in Cc. Upon such confirmation, D4233 changes the staff member’s status in the registration tool from “place” to “closed”.

The crèche sends D4233 regular updates on occupancy and D4233 updates the registration tool accordingly. The updates from the crèches are word or excel files. These are deleted 1 year after the end of the crèche year

External crèche Kita Haar
The registration process runs outside the registration tool. The parents contact D4233 directly in case of interest in the external crèche. D4233 informs KiTa Haar by email providing name and surname of the staff member and child and announces the registration. The parents then contact the KiTa Haar directly and conclude the contract. The EPO pays a place fee.

The registrations are recorded in an excel list, which is deleted 1 year after the termination of the childcare.

Data Retention Data stored in the registration toll are deleted after 1 year the child has left the crèche.

Emails stored in Outlook for the processing of the requests are deleted after 1 years from the date on which the email is sent.

Purpose of Processing The purpose is to process staff members’ requests for a place in the Munich in-house/external crèches and to allocate the places to the eligible persons.

Data subjects and categories of personal data

Employees

Contact Information	
Contact Details	Home Address

Phone Numbers	Working email address
Family Information	
Children's Names	Child's birthday
Spouse's name	

Externals

Contact Information	
Contact Details	Working email address

Recipient of the personal data

Recipients of the data AWO-Isar
AWO-Pschorr
Merlin
KiTa Haar

BIT might have access to the data for technical support or/and IT service maintenance

Statistics could possibly be requested by management, but these would only contain anonymised data.

Purpose of sharing

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 179

Name Consultation with the Ombuds Office - external clients

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 045 - Internal Audit and Professional Standards - Ombuds Office

Entity Name - Processor (Entities)

Description of the processing

Description - Client raises a matter with the Ombuds Office.
- In-take of the case data: The confidential treatment of the data provided by the client is also explained in the DPS as follows:

"When you contact the Ombuds Office, your matter will be treated in the strictest of confidence. Your data will be shared confidentially with the appropriate EPO managers, who will receive the minimum information essential to deal with your matter. Should the Ombuds Office consider it necessary to share your personal data with any other EPO staff involved in your matter, it will do so only with your express agreement.

Once your matter is closed, all personal data, including any reference to your organisation or affiliation or to the applicant you are representing, will be deleted. You can close your matter at any time, in which case all personal data, including any reference to your organisation or affiliation or to the applicant you are representing, will be deleted.

The Ombuds Office will keep an anonymous record of reported matters to enable it to identify trends or systemic issues. Its reports will not contain any details relating to personal data or to organisations or affiliations.

In exceptional cases, where the Ombuds Office considers information shared with it to indicate an imminent risk of serious harm to an individual or an illegal activity, it will share this information with relevant EPO managers to enable them to take appropriate action. If your matter relates to an integrity issue, such as fraud, corruption or other irregular activities, you should report it to the EPO department responsible for ensuring compliance at investigations@epo.org or at + 49 89 2399 1577.

You may inform the Ombuds Office at any time that you do not wish to continue the procedure with the Ombuds Office. In this case, your personal data, including any reference to your organisation or affiliation or to the applicant you are representing, will be deleted and any other data you have provided will be anonymised.

Please be reassured that your personal data will be processed solely for the above-mentioned purposes. In addition, the processing is not intended to be used for any automated decision making, including profiling. Your personal data will not be transferred to recipients outside the EPO."

Data Retention Any personal data, including reference to organisation, affiliation or representation, collected during a consultation with a client will be deleted upon confirmation from the client that the matter is closed.

Anonymised non-case related data will be retained and used to generate systemic and trend data for reporting and general quality improvement actions.

Purpose of Processing Personal data are processed with the purpose of assisting that the client in getting their matter back on track when the regular formal channels have been unable to resolve the matter to their satisfaction. The Ombuds Office will also maintain an anonymous record of reported matters so that it can identify trends or systemic issues. Its reports will not contain any details relating to personal data or organisations or affiliations.

Data subjects and categories of personal data

Employees

General	
Any other information	Assessment and legal opinions
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Contact Information	
Contact Details	Mobile Phone Number
Personal Email	Phone Numbers
Private Phone Number	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Personal data potentially included within the content of patent procedure related information and publications	
Employment Information	
Assessment and legal opinions	Business Unit Division
Department name and/or number	Job Title Role
Office Location	
Personal Identification	
Digital signature	First Name
Full Name	Surname

Externals

General	
Any other information	User association

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Contact Information	
Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Working email address
Professional Experience & Affiliations	
Affiliation	Professional Memberships
Representation in EPO’s Patent Granting Process	
Affiliation to Association of professional representatives	Role in the Patent Grant Procedure
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Personal data potentially included within the content of patent procedure related information and publications	
Employment Information	
Business Unit Division	Company Entity
Department name and/or number	Job Title Role
Office Location	
Personal Identification	
Digital signature	First Name
Full Name	Surname
Signature	

Recipient of the personal data

Recipients of the data When you contact the Ombuds Office, your matter will be treated in the strictest of confidence. Your data will be shared confidentially with the appropriate EPO managers, who will receive the minimum information essential to deal with your matter. Should the Ombuds Office consider it necessary to share your personal data with any other EPO staff involved in your matter, it will do so only with your express agreement.

Purpose of sharing cf. comments to 1.6

When you contact the Ombuds Office, your matter will be treated in the strictest of confidence. Your data will be shared confidentially with the appropriate EPO managers, who will receive the minimum information essential to deal with your matter. Should the Ombuds Office consider it necessary to share your personal data with any other EPO staff involved in your matter, it will do so only with your express agreement.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet
https://www.epo.org/about-us/office/data-protection-and-privacy/ombuds-office.html

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 182

Name Disposal of e-waste

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

Entity Name - Processor (Entities)

External processors

PlanBit

External processors	
Name PlanBit	

Description of the processing

Description In the context of the EPO's environmental sustainability goals and in particular the EPO's target to be carbon neutral by 2030, the eWaste (ITAD) service for ICT assets and electronics has been put in place to provide a single point of disposal service for any brand and multi types of ICT asset owned by the EPO, managing ICT assets disposals in an ethical and sustainable way and contributing, amongst others, to end-of-life responsible recycling and upcycling and reduction of e-waste and thus contributing to a more circular business economy.

In that context, personal data is processed as follows:

1) For the management of the contract, processing of personal data will be limited to the contact details (Name/Surname; work e-mail; work phone numbers) of the EPO staff authorised to manage the contract

2) For the performance of the contract, in particular the sanitisation of any data bearing devices, personal data processing (i.e. destruction or data erasure / complete and irreversible deletion or data wiping)) could theoretically include any kind of personal data stored on the media.
The service therefore provides for an end-to-end tracing of the hardware media and data, including GPS tracking from the moment equipment is collected at the EPO, serialized recording upon arrival at the facility, detailed traceability for data bearing devices, detailed end reports for all devices and traceability after processing (reuse or recycling).
Deletion is done according to the NIST 800-88 standard.
The deletion processes are automated, i.e. the technicians don't access the personal data in order to delete it.
If deletion attempts are unsuccessful, the data media will be built out and shredded

Data Retention 1) For the management of the contract, data will be retained for the duration of the contract.
2) For the performance of the contract, no personal data will be retained (as the purpose is to erase / delete the data). Certificates of data removal will be kept for 5 years (no personal data in scope here).

Purpose of Processing 1) Management of the contract with PlanBit., 2) Performance of the contract, in particular the sanitisation of the information media (i.e. destruction or data erasure / complete and irreversible deletion or data wiping).

Data subjects and categories of personal data

Contractors

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact

Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Thermal Information	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
General	
Assessment and legal opinions	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Emergency Contact Details

Home Address	Personal Email
Phone Numbers	Previous Residence Address
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Correspondence	
Personal information provided voluntarily	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
Ticketing	
Ticket related data	
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Appeals Records Information	Assessment and legal opinions
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Disciplinary Action	End Date
End Date and Reason for Termination	EPO access badge number

Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Title Role
Language preference (of communication)	Line Reporting Manager
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Room Number	Salary
Start Date	Weight
Unknown	
EPO badge validity	Price list for discounts
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session details	
Health Data	
Health Data	
Professional Experience & Affiliations	
CV	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Financial	
Bank Account Information	Bank Account Number
Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans

Insurance Information	Routing Number
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
User Account Information	
Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	
Driving Licence Number	National Identification Number
National Identity Card Details	Passport Number
Social Security Number	

Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Thermal Information	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	

Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
General	
Assessment and legal opinions	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Home Leave Address
Personal Email	Phone Numbers
Previous Residence Address	Teleworking address
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
Diagnostic tools’ results	IDP
Instructor related data	Learning external events
Learning history	Learning plan

Ratings	Social learning inputs
Correspondence	
Personal information provided voluntarily	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
Ticketing	
Ticket related data	
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Appeals Records Information	Assessment and legal opinions
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Disciplinary Action	End Date
End Date and Reason for Termination	EPO access badge number
Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Title Role
Language preference (of communication)	Line Reporting Manager
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave

Room Number	Salary
Start Date	Weight
Unknown	
EPO badge validity	Price list for discounts
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session details	
Health Data	
Health Data	
Professional Experience & Affiliations	
CV	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Family Information	
Children's Names	Child's birthday
Parents' Names	Spouse's information
Spouse's name	
Financial	
Bank Account Information	Bank Account Number
Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History

Website History	
User Account Information	
Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	
Driving Licence Number	National Identification Number
National Identity Card Details	Passport Number
Social Security Number	

Externals

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Ticketing	
Ticket related data	
Sensory and Electronic Information	
Audio Information	Electronic Information
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Biometric	
Facial Recognition	Voice Recognition
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	
Business Unit Division	Company Entity

Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	End Date
EPO access badge number	Hours of Work
Job Title Role	Language preference (of communication)
Office Location	Previous Work History
Unknown	
EPO badge validity	Price list for discounts
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Network/application Interaction Data	
Session details	
Health Data	
Health Data	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Personal Email
Phone Numbers	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data

IDP	Instructor related data
Learning external events	Learning history
Learning plan	Ratings
Social learning inputs	
Professional Experience & Affiliations	
CV	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
European Patent Register Data	
Address	Data provided by the data subjects
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Personal data potentially included within the content of a patent (claims, description, drawings, abstract)	
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
User Account Information	
Account Age	Account Number
Account Password	
Government Identifiers	
National Identity Card Details	Passport Number

Former Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Thermal Information	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Workplace Welfare	

Records of Personal Properties	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Home Leave Address
Personal Email	Phone Numbers
Previous Residence Address	Teleworking address
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Correspondence	
Personal information provided voluntarily	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
Ticketing	
Ticket related data	
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Appeals Records Information	Benefits and Entitlements Data
Business Unit Division	Company Entity

Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	Disciplinary Action
End Date	End Date and Reason for Termination
EPO access badge number	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Title Role	Language preference (of communication)
Line Reporting Manager	Military Status
Office Location	Performance Rating
Personnel Number	Previous Work History
Record of Absence/Time Tracking/Annual Leave	Salary
Start Date	Weight
Unknown	
EPO badge validity	Price list for discounts
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Session details	
Health Data	
Health Data	
Professional Experience & Affiliations	
CV	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name

Financial	
Bank Account Information	Bank Account Number
Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browsing Time	Cookie Information
IP Address	Network Interaction History
Website History	
User Account Information	
Account Age	Account Number
Account Password	Password
User ID	
Government Identifiers	
Driving Licence Number	National Identification Number
National Identity Card Details	Passport Number
Social Security Number	

Prospective Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Ticketing	
Ticket related data	
Sensory and Electronic Information	
Time stamps from their access to the buildings	

Building area and site	
Building area and site	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Department name and/or number	End Date
End Date and Reason for Termination	EPO access badge number
Grade	Job Application Details
Job Title Role	Language preference (of communication)
Line Reporting Manager	Military Status
Office Location	Performance Rating
Previous Work History	Salary
Start Date	Weight
Unknown	
EPO badge validity	Price list for discounts
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status

Nationality	Picture
Religion/Religious Beliefs	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Network/application Interaction Data	
Session details	
Health Data	
Health Data	
Contact Information	
Contact Details	Emergency Contact Details
Home Address	Personal Email
Phone Numbers	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Professional Experience & Affiliations	
CV	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Correspondence	
Personal information provided voluntarily	
Financial	
Fund Reservation Requests	Information on home loans
User Account Information	
Account Age	Account Number
Account Password	Password

Government Identifiers	
National Identity Card Details	Passport Number

Recipient of the personal data

Recipients of the data Staff from D463 and PlanBit

Purpose of sharing Management of the contract (notification of equipment for collection, reporting on devices erased / deleted / recycled / reused).

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures
Technical and organisational measures of PlanBit are described in the DPA. PlanBit is certified ISO27001 (and ISO 9001 + ISO 14001). Standard procedure for data removal is NIST-800-88 Purge, EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 184

Name Applications and patents related Legal advice

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Atlassian/JIRA tool

External processors	
Name Atlassian/JIRA tool	

Microsoft

External processors	
Name Microsoft	

Global Lingo

External processors

Name
Global Lingo

OpenText

External processors
Name
OpenText

ServiceNow

External processors
Name
ServiceNow

Description of the processing

Description Upon request from EPO staff and, in selected case, from externals, D 5.2.1. provides legal and procedural advice in the form of explanatory notes, legal opinions or internal notes to specific applications or patents, drafts for legal texts, presentations, letters, speaking notes etc. (hereinafter “legal advice”). It includes replies to external enquiries not related to specific applications/patents, forwarded to D521 by EPO Customer Support via their tool (CSM/ServiceNow).

Personal data processed in this operation, if any, is provided by the requester.

All requests are registered in the case management system (Mattersphere or JIRA) under a specific Log number together with the requester’s and responsible officer’s names and assigned to the case handler within the Directorate.

Once the request has been assigned to the case handler the legal question is identified, assessed, and answered to the requester.

Receipt of the request, its processing and the provision of the reply may occur via e-mail, via chat functions or by any other tool available for intra-Office communication collaboration. The correspondence, drafts and final legal advice are saved in the CMS.

It might be necessary, during the elaboration of the advice, to consult other units of the Office, which might require the sharing of relevant personal data with them by email, by giving access to the document on a shared drive or by any other suitable means. This might also result in the further processing of personal data of staff members involved. In certain cases, such as publication in the official journal, amendment of EPC regulations, the tool OpenText/Common log is used for internal communication.

In the course of the above mentioned activities, it is also regularly necessary to record witness hearings during oral proceedings of the legal division involving D 5.2.1 is a member,

The active handling of a case stops when the entry in the CMS is closed in accordance with the applicable internal procedures.

This record covers also related organisational measures within the delegated controller's unit e.g. internal meetings, minutes' taking.

The personal data is kept until the end of the applicable retention periods.

Purpose of Processing 1. The processing of personal data is necessary for providing legal advice on matters within the responsibility of Legal Affairs/D 5.2.1, mainly providing legal and procedural advice in patent law related matters, providing up-to-date information to stakeholders as well as all associated actions to e. g. ensure a proper and efficient information flow and management of associated activities., 4. Ensuring proper collaboration, consultation, alignment and hierarchy’s approval, 3. Deliver required advice, ensure proper preparation of subsequent actions (e.g. further communications, oral proceedings, final decision),, 5. preparation of statistics and overview for reporting purposes, 6. retrieval of previous advice as precedence, example and reference when dealing with new requests, with a view to harmonise internal and external practice., This encompasses: 2. Registering incoming requests,

Data Retention Personal data for non patent-file related matters is kept for the default retention time period for legal advice of Legal Affairs (20 years) except for cases where e. g. President, Vice President or other high ranked Officers were involved in order to be able to document the decision-making process.

Personal data in patent-file related matters (European patent applications and European patents) should be kept for thirty years to cover the longest possible period under Rule 147 EPC.

Data subjects and categories of personal data

Employees

General	
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Matter/Log file	
Attachments	Metadata
Ticketing	
Ticket related data	
Contact Information	
Contact Details	
Correspondence	
Additional Information which might be provided in the course of exchanges	
Employment Information	
Business Unit Division	Department name and/or number
Job Title Role	Office Location
Personal Identification	
Full Name	Gender

Externals

Matter/Log file	
Attachments	Metadata
General	
Any other information	

Ticketing	
Ticket related data	
Contact Information	
Contact Details	
European Patent Register Data	
Address	Data provided by the data subjects
Representation in EPO's Patent Granting Process	
Role in the Patent Grant Procedure	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Employment Information	
Company Entity	
Personal Identification	
Digital signature	Full Name
Gender	Signature

Recipient of the personal data

Recipients of the data 1) Requester 2) EPO hierarchy (above the delegated controller) 3) other units	**Purpose of sharing** 1) Requester (internal or external), who contacted legal affairs in the first place to obtain e.g. an advice 2) Hierarchy (when applicable) when the circumstances of a case require their information and/or decision. 3) other units (in some cases, colleagues from other units in the Office might need to be involved, on a need-to-know basis), as necessary to address a particular matter.

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) Global Lingo - United Kingdom, Microsoft - United States, OpenText - United States, ServiceNow - Australia, ServiceNow - United States, ServiceNow - India, ServiceNow - Japan, ServiceNow - United Kingdom, TRE Thomson Reuters - Luxembourg

Transfer to public authority and/or International Organisation 1) National Patent Offices
2) International Organisations such as WIPO
3) European institution such as EUIPO, CVPO

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities, Public Authorities/Government Bodies

Transfer mechanism(s) The recipient provided appropriate safeguards, Legally binding and enforceable instrument between public authorities or bodies, A derogation in accordance with Art. 10 DPR

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 205

Name Splunk

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

Entity Name - Processor (Entities)

External processors

Umbrio

External processors	
Name Umbrio	

Description of the processing

Description Splunk is a central log repository for security incident management enabling systems' protection by helping identify and analyse security issues.
The processing comprises (a) receiving technical data generated and already available from other BIT systems and services (b) performing automated queries for generating alerts for relevant security events (c) performing automated queries for generating dashboards and overviews of security relevant information
(d) performing manual queries for deeper analysis of security events, adaptation of dashboards and alerts.

Splunk receives technical data generated on (and available on) a number of EPO systems and services, in particular:
a. EPO-managed workstations assigned to EPO users
b. EPO-managed Servers
c. EPO-managed network equipment (e.g. routers, switches, firewalls, proxy servers)
d. External cloud providers with an established contractual relationship with the EPO (e.g. Microsoft, Google, Amazon, SAP)

Data Retention Data which is stored on servers in Luxemburg is subject to the regular backup and archiving retention policy for on-premise servers. Splunk log files are stored automatically and are kept for an agreed period of time depending on the type of information and the system to which it refers. Microsoft Defender for Endpoint Security alert/incident related data is retained for 12 months within Splunk. Data is kept in Splunk for up to 18 months, after which it is automatically deleted. Data is kept in backups for 60 days after expiration from Splunk system, after which it is no longer available.
As a result, Splunk's overall data retention never exceeds 20 months.

Purpose of Processing Personal data is processed for the purposes of being able to identify the persons that carried out the activities that have been logged, in order to address any possible error or security incident that is detected. This is important because: • Log files are used to trace events in an information system and to help debugging and repair. They are part of the systems and are essential tools to provide the security and an efficient support when information systems are not working correctly. • Log files of EPO systems are processed for investigation and elimination of security incidents and malware infections on devices connected to the EPO network, and/or for prevention of data leaks. • Additionally, log files might be processed for statistical purposes or eliminating problems with users' access to EPO telecommunications systems. Any request for analysis of Splunk data other than to ensure the security and stability of EPO systems requires a separate, specific consultation with the DPO.

Data subjects and categories of personal data

Contractors

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	
Network/application Interaction Data	
Session metadata	
Ticketing	
Ticket related data	

Physical and/or Digital Identifiable Assets	
Operating System Version	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Contact Information	
Phone Numbers	Working email address
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	IP Address
Network Interaction History	URL
Website History	
Employment Information	
Active/Inactive Indicator	Contract Type
Department name and/or number	End Date
Job Title Role	Language preference (of communication)
Line Reporting Manager	Office Location
Personnel Number	Room Number
Start Date	
Personal Identification	
First Name	Full Name
Gender	Surname
Geolocation	
Geolocation Information	
User Account Information	
Account Number	User ID
System Logs	

Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	

Employees

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	
Network/application Interaction Data	
Session metadata	
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Operating System Version	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Contact Information	
Mobile Phone Number	Phone Numbers
Working email address	
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	IP Address
Network Interaction History	URL

Website History	
Employment Information	
Active/Inactive Indicator	Contract Type
Department name and/or number	End Date
Job Group	Job Title Role
Language preference (of communication)	Line Reporting Manager
Office Location	Personnel Number
Room Number	Start Date
Personal Identification	
First Name	Full Name
Gender	Surname
Geolocation	
Geolocation Information	
User Account Information	
Account Number	User ID
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	

Externals

Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	
Network/application Interaction Data	

Session metadata	
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Operating System Version	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	IP Address
Network Interaction History	URL
Website History	
System Logs	
Firewall/Router/Switch Logs	System-, Application-, Security-related Server Logs
Web Servers Logs	

Recipient of the personal data

Recipients of the data The only users of Splunk within PD 46 are BIT Information Security department and BIT Network and Data Centre Management department. All use of Splunk is to support security and network use cases, in abidance with need-to-know principle.
If other recipients request access to the personal data, this will be individually asked to the Delegated Controller consulting DPO for advice.

Purpose of sharing The purpose of sharing Splunk personal data to BIT Information Security and BIT Network and Data Center Management recipients is to cover the requirements of EPO's IT security and network use cases.
Any personal data can be processed as part of preventative, reactive and explorative use cases in compliance to the need-to-know principle, in so far as this is required to allow BIT support services to identify and locate the relevant systems and/or users. Explorative use cases are intended only for the purposes of identifying and fine-tuning new preventative or reactive use cases.

Any eventual request to analyse Splunk data having a purpose other than ensuring EPO systems' security and stability would require the preliminary, specific and separate consultation with the DPO.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures Access Control - All queries using Splunk are done by authenticated users. Authentication is based on the EPO Active Directory systems, thereby ensuring that the normal account lifecycle management (such as deactivation of accounts for staff no longer in service) is implemented. - Access to Splunk is role-based. Active Directory groups govern which role/s a user belongs to, and roles are restricted in the type of information they can see in Splunk. -Only members of BIT Information Security and Network and Data Center Management departments can query data indexes containing personal data. Audit Trail -Splunk maintains a full audit trail of user queries and other activity. -The information, like any other information in Splunk, is “append only” so once written it cannot be altered or removed undetectably., EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet work in progress

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 210

Name European Inventor award - Ceremony

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 02 - Communication

Entity Name - Processor (Entities) DG1 - 1 - Patent Granting Process, DG4 - 41 - Finance, DG4 - 45 - CTO / BIT, DG4 - 47 - Procurement and Vendor Management

External processors

Huddle

External processors	
Name Huddle	

Amazon Web Services (AWS)

External processors	
Name Amazon Web Services (AWS)	

Description of the processing

Description In the context of the European Inventor Award and Young Inventors prize, personal data are processed by the EPO in the following situations:

Nominating the inventors and the finalists.
Personal data are collected when the applicant completes the online nomination form provided on the EPO website.
Inventors' personal data are shared internally within the EPO and a pre-selection is made.
The processing is also necessary for deciding on the composition of the jury. Personal data of the

selected inventors are then shared with the jury. The EPO processed personal data about the jury members for their appointment as well as for the organisation of the meetings in which the jury members will select the finalists and winners. The rest of the selection process is performed by the jury. The jury decides who the finalists are.
For the Young Inventors Prize, the EPO will handle with the utmost care any children's personal data processed, such as pictures, video recordings or related information used for the evaluation of their applications and their possible participation in the event as a finalist. The EPO ensures that all necessary steps are taken to protect children’s interests, rights and freedoms when processing their personal data.

Selecting the finalists and winners
The jury deliberation meetings are carried out through MS Teams. In order to ensure that the selection procedure is accurate, as well as for minute-taking purposes, the meeting is recorded. Excerpts of the recording, as well as quotes from the participants might be published on the EPO website to create visual content for the promotion of jury’s participation in the event.

Holding the ceremony
EPO collects personal data directed from the nominees and process them to organise the ceremony. Personal data might be shared with the external providers entrusted with the organisation of the ceremony, travels and accommodations. After the ceremony, only the necessary data is kept in the EPO databases.
Public in general can attend the ceremony by streaming and personal data may be collected through the streaming platform for statistical purposes.
During the event, data subjects may have the possibility to actively participate in diverse ways. For example, by being part of the videos that the EPO may create for the ceremony together with the videos of the finalists or by interacting with the emojis provided in the landing page of the event or through the different social media where the EPO is present. Personal data about the online interactions may be collected for statistical purposes.
When the ceremony is held in presence, personal data processing may also be necessary for logistics support before (e.g. for managing the registration, accommodation and the provisioning of meals) during and after the ceremony. In such cases, the processing may include health related data.

Promoting the European Inventor Award and Young Inventors prize and the ceremony.
The EPO promotes the Award externally, and each year the EPO develops new ways of interacting with the public according to the trends on social media platforms and the technology.
Personal data are processed for sending information about upcoming Award, such as event invitations and reminders, the EPO shares your email address with an external provider that supports us with the mailing lists. If you are receiving these emails, it is because your personal

Purpose of Processing Maintenance and operational support, Organisation of meetings and the ceremony, Appointment of the jury members, Promotion of the competition and the ceremony, Creation of the promotional material, Nomination and selection of the inventors

data are part of a database shared internally among EPO departments in order to inform data subjects about future meetings or events.
We obtained the personal data from your registration at past events or from other sources (publicly accessible sources, another participant in a meeting/event entitled to provide data on your behalf, etc.). Data subjects are given the possibility to opt-out.
For the promotion of the Award through different social media and press media communication channels, the EPO collects additional personal data from the finalists, jury members and other participants that may appear in the audio-visual material, and which is shared among different multipliers such as media agencies, influencers and European institutions. This audio-visual material is used not only to promote a specific edition of the Award, but also the Award as such and other EPO related Intellectual Property activities and events.
Personal data from EPO staff, jury members and stakeholders are also processed if they take part to the creation of the promotion material.
The EPO may organise voluntary activities among the EPO employees, so that both the Award and the staff engagement are promoted. For example, EPO employees could be enrolled in the production of a promotional video or be part of the audience at the ceremony.
Social media plugins and embedded YouTube videos are put in place not only on the web pages used to promote the event, such as the epo.org, the inventoraward.org and the Popular Prize microsite, so that people can promote the event through their personal accounts.

Data Retention Once each edition ends, the external providers will delete any personal data processed from their files after having returned them to the EPO in accordance with the data protection agreements they have signed with the EPO.

Personal data about the inventors who are nominated one year may be also selected as a finalist in another year. To identify and encourage people to continue nominating candidates each year, and to be able to evaluate the development of an invention or an inventor’s career, personal data of the person nominating, and the nominee provided in the nomination form are kept for a maximum of five years.

The personal data associated with the organisation of the Jury meeting will be erased the latest after 6 months following the last action in relation to the event. Nevertheless, in accordance with the data protection statement of the organisation of the jury meeting, some personal data needed for the promotion of the event might be kept for a longer period of time.

When you vote for the Popular Prize, all your personal data are directly anonymised, except for the name of the inventor you voted for. The anonymised data are only used for statistical purposes. The external provider will delete the collected data from their database two weeks after

the close of the voting procedure, which is on the day of the event. However, please bear in mind that cookies might be kept on your device for a longer period.

The personal data associated with the organisation of the ceremony and its promotion in the form of staff and user engagement activities must be erased within two years of the last action related to the event. Nevertheless, some personal data may be kept for up to 25 years for educational, institutional, historical, informational and/or (internal and external) promotional purposes. Personal data published on the EPO's internal and external channels, such as EPOtv and the EPO website, or made available via other social media channels used by the EPO, such as YouTube, LinkedIn, Instagram and Facebook, will be limited as much as possible, for example by storing only the names, surnames and photos/videos of finalists and other participants in the ceremony.

If as a finalist agrees to be contacted for other activities relating to the EPO and join any future alumni network, the EPO will retain details such as biographical data and email address for as long as you agree to be part of that network.

If data subjects have subscribed to any EPO newsletter, the privacy statement for the EPO's newsletters and related alerts applies.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

Data subjects and categories of personal data

Externals

Social	
Social Media Account	Social Media Contact
Sensory and Electronic Information	
Audio Information	Presence Status
Time stamps from their access to the buildings	Visual Information
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	
Active/Inactive Indicator	Company Entity
Department name and/or number	Duration of employment

Job Title Role	Language preference (of communication)
Office Location	Previous Work History
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	
Education & Skills	
Educational Degrees	Languages
General	
Answers to surveys, assessments or quizzes	Any other information
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number
Working email address	
Professional Experience & Affiliations	
Affiliation	CV

Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Financial	
Bank Account Information	
Browsing Information	
Browsing Date and Time	Cookie Information
IP Address	URL
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	

Employees

General	
Any other information	
Contact Information	
Contact Details	Country
Mobile Phone Number	Teleworking address
Working email address	
Building area and site	
Building area and site	

Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Employment Information	
Contract Type	Department name and/or number
Duration of employment	End Date
Job Group	Job Title Role
Language preference (of communication)	Line Reporting Manager
Office Location	Record of Absence/Time Tracking/Annual Leave
Room Number	Start Date
Personal Identification	
Age	First Name
Full Name	Gender
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	
Education & Skills	
Education and Training History	Languages
Project management experience	

Contractors

Health Data	
Dietary requirements	Health Data
Mobility needs	
Sensory and Electronic Information	
Visual Information	
Professional Experience & Affiliations	
CV	

Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Employment Information	
Company Entity	Contract Type
Department name and/or number	Job Title Role
Line Reporting Manager	Office Location
Personal Identification	
Full Name	Gender
Nationality	
User Account Information	
Ownership Permissions	
Education & Skills	
Languages	
Government Identifiers	
National Identification Number	

Recipient of the personal data

Recipients of the data The EIA team composed by EPO staff and external contractors have access to the data. In addition, some colleagues from Principal Directorate Communication and other departments such as DG1 have also access, so that they can support the EIA team on the analysis of the nominated patent or the promotion of of the ceremony. Personal data may be disclosed to third-party service providers for the purpose of organising the event, creating and promoting the campaign, maintaining and supporting the platforms created for the nominations, the event and the Popular Prize, and ensuring compliance with security and health-related standards. Additionally, the audiovisual material produced may be shared with other public entities for promotional purposes, and with the public in general through the EPO social media accounts and website. In general, promotional material is shared with the genepublic via several communication channels.	**Purpose of sharing**

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Huddle - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Service provider processing data for the creation of statistics, Sub-processor(s) storing the personal data

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted on EPO premises, most of the external providers supporting the EPO generally commit in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has carried out a privacy and security risk assessment. These systems are required to have implemented appropriate technical and organisational measures such as: physical security measures, access and storage control measures, securing data at rest (e.g., by encryption); user, transmission and input control measures (e.g., network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging); conveyance control measures (e.g. securing data in transit by encryption).

Data protection statement

Data Protection Statement link internet - Nomination & Ceremony: https://inventoraward.epo.org/privacy-policy & https://www.epo.org/about-us/office/data-protection-and-privacy.html#DPS%20for%20EIA%20and%20YIP
- Popular Prize: https://popular-prize.epo.org/data-protection-privacy
- Jury members (provided through email)

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 215

Name Videoconferencing via Zoom

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

Entity Name - Processor (Entities)

External processors

Zoom

External processors	
Name Zoom, Zoom	

Description of the processing

Description Zoom Video Communications ("Zoom") is a cloud-based videoconferencing (VICO) platform enabling the - successful - organisation of events in a virtual environment such that effective interaction between participants is as close as possible to a face-to-face experience.

With a view to the needs of the Office and its stakeholders to continue enjoying access to all services the EPO has extended the use of videoconference in order to organise virtual events. Within this framework, Zoom is used for conducting such virtual events, in particular for events where simultaneous interpretation is required, such as for example oral proceedings or board meetings with Member States (AC, BFC, etc.)

Personal data is processed in the Zoom platform for the purpose of carrying out the virtual event and ensuring the effective collaboration and communication between the Office and its stakeholders thus guaranteeing EPO business

operations and compliance with applicable legal obligations. The collected data may also be used to prepare anonymised statistics on the meetings and participants such as type of meeting, number of meetings, average duration, meeting interruptions and reconnections, etc. for quality and volume monitoring purposes.

In addition, Zoom may process some personal data for its own Legitimate Business Purposes, as an independent Controller, solely when the processing is strictly necessary and proportionate and for one of the following purposes: a) directly identifiable data for the purposes of - billing, account and customer relationship management and relating correspondence - complying with and resolving legal obligations - abuse detection, prevention and protection, virus scanning and scanning to detect violations of terms of service and b) pseudonymised and/or aggregated data for - improving and optimising the performance and core functionalities - internal and financial reporting, revenue and capacity planning, forecast modelling - receiving and using feedback for overall service improvement.

Personal data eventually present in Zoom may be subject to additional processing operations done according to other purposes.

As part of the nature of a collaborative tool, additional personal data may be included in the information that is exchanged between meeting participants during a particular meeting or event, such as instant messages (chat), images, files, whiteboards, transcripts and recordings. Any such purposes are established by the organisational unit to which a specific user belongs to, represented by the Delegated Controller of the organisational unit.

Recordings via Zoom are done only if strictly necessary for legitimate and explicit purposes and approved in advance; default setting is that no one can record. The user is automatically notified when a recording starts and will be given the option to leave the virtual event in case he/she does not wish to be recorded.

Data Retention Zoom shall retain the personal data of the attendees strictly necessary for the organisation and management of a particular event/meeting for the maximum of one month.

Purpose of Processing Personal data is processed for the purpose of conducting videoconferences / virtual events organised by the EPO.

Data subjects and categories of personal data

Contractors

General	
Answers to surveys, assessments or quizzes	
Network/application Interaction Data	
Session metadata	

Physical and/or Digital Identifiable Assets	
Mobile Device Name	Mobile Device's Network Adapter MAC Adress
Operating System Version	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Contact Information	
Contact Details	Country
Phone Numbers	Working email address
Device Management Data	
Account ID	MAC Address
Platform-specific IDs	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Personal information provided voluntarily	
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Cookie Information	IP Address
URL	
Geolocation	
Geolocation Information	

Employees

General	
Answers to surveys, assessments or quizzes	
Network/application Interaction Data	
Session metadata	
Physical and/or Digital Identifiable Assets	
Mobile Device Name	Mobile Device's Network Adapter MAC Adress

Operating System Version	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Contact Information	
Contact Details	Country
Phone Numbers	Working email address
Device Management Data	
Account ID	MAC Address
Platform-specific IDs	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Personal information provided voluntarily	
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Cookie Information	IP Address
URL	
Geolocation	
Geolocation Information	

Externals

General	
Answers to surveys, assessments or quizzes	
Network/application Interaction Data	
Session metadata	
Physical and/or Digital Identifiable Assets	
Mobile Device Name	Mobile Device's Network Adapter MAC Adress
Operating System Version	Workstation's Hostname (Physical or Virtual)

Workstation's Network Adapter MAC address	
Contact Information	
Contact Details	Country
Phone Numbers	Working email address
Device Management Data	
Account ID	MAC Address
Platform-specific IDs	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Personal information provided voluntarily	
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Cookie Information	IP Address
URL	

Former Employees

General	
Answers to surveys, assessments or quizzes	
Network/application Interaction Data	
Session metadata	
Physical and/or Digital Identifiable Assets	
Mobile Device Name	Mobile Device's Network Adapter MAC Adress
Operating System Version	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Contact Information	
Contact Details	Country

Phone Numbers	Working email address
Device Management Data	
Account ID	MAC Address
Platform-specific IDs	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Personal information provided voluntarily	
Telephony Interaction Data	
Telephony Session Metadata	
Browsing Information	
Browser type	Browser User Agent
Cookie Information	IP Address
URL	
Geolocation	
Geolocation Information	

Recipient of the personal data

Recipients of the data - EPO Staff and external users
- Members of the department 4615 PACE
- Zoom

Purpose of sharing The personal data is disclosed, on a need to know basis, to the following recipients:

- the EPO's staff members and external users participating in or organising virtual events;
- Members of the department 4615 - PACE (Productivity Apps, Collaboration &Events)
- Zoom and its third-party providers for service maintenance and support purposes.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) Zoom - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures Zoom has SOC 2 type II certification for compliance with security, availability, processing, integrity and confidentiality standards and its cloud services provider is ISO 27001 certified., EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 217

Name EQE - European Qualifying Examination

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 51 - Cooperation and Patent Academy

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

UNIwise

External processors	
Name UNIwise	

G.A.S.T

External processors	
Name G.A.S.T	

Description of the processing

Description Personal data is processed by the EPO to successfully organise and manage the European Qualifying Examination and follow-up actions in accordance with Article 134 EPC and the Regulation on the European qualifying examination (REE) and its Implementing provisions (IPREE).

The present document aims at providing information on how the personal data are processed in the context of the different stages and activities of the EQE, such as the registration and enrolment of the candidates, the correct performance of the examination, the provision and publication of the result and the appeals as well as

the selection and appointment of the Committees members.

The examination is organised and conducted by a Supervisory Board, an Examination Board, Examination Committees and an Examination Secretariat. The composition and duties of the bodies as well as the procedures to appoints their members are regulated in the REE (Articles 2 to 10) and IPREE. The names of the members are published online once they have been appointed by the President.

Members of the Supervisory Board, Examination Board and Examination Committees provide their data when applying to become member of the respective body. The information is entered into the system by the Examination Secretariat.

According to Rules 1 and 28 IPREE and Article 11 REE, candidates intending to enrol for the European qualifying examination (EQE) for the first time must register once they have commenced their professional activity within the meaning of Article 11(2) REE. Candidates must upload all supporting documents to the web portal: documentation that proves their identity, academic qualifications and professional requirements. When required, paper documents are entered into the systems by the Examination Secretariat.

Formal requirements are assessed by the Examination Secretariat, who decides on the registration and enrolment of candidates in accordance with the REE and the IPREE. The Examination Secretariat checks if the formal requirements are met and, in case of doubt, asks the provider of the data for further evidence.

These activities include the processing of personal data for the registration for the assessment of special cases (disabilities), for the candidates' enrolment as well as for the payment of the fees. Candidates with disabilities are flagged in the system as needing special arrangement, the medical details of the disability as such are not named nor stored, since only compensation is offered. Correspondence with candidate is kept in his/her file as long as the candidate is active in the EQE.

The exam can be done via an online platform or in presence.

The external supplier that provides the online platform process personal data on the EPO's behalf and it is in charge of the maintenance of the platform and offering support. The online platform has proctoring features to monitor the candidates during the examination to prevent attempts of fraudulent behaviour and keep proof of them, where deemed necessary.

The answers are marked, and the results provided by the markers via the online portal and verified by the Examination Board. The results are made available by the Examination Secretariat to each candidate together with the marking sheets

Purpose of Processing Personal data is processed by the EPO to successfully organise and manage the European Qualifying Examination and follow-up actions in accordance with Article 134 EPC and the Regulation on the European qualifying examination (REE) and its Implementing provisions (IPREE).

pertaining to his answer papers.

According to Article 21 REE, candidates' anonymity shall be respected when their answers are marked and their answers may be published for research, statistical or training purposes provided their anonymity is respected.

The appeal procedure before the Disciplinary Board of Appeal under Article 24 REE. follows the rules before said Board and the additional Rules of Procedure of the Disciplinary Board of Appeal of the European Patent Office.
The texts of these Rules, the business distribution schemes of the Boards and other information on the Boards and the appeals procedures are contained in the annual supplementary publication to the EPO Official Journal "Information from the Boards of Appeal".

Data Retention Reasons are explained in the Annex: Archiving and Retention policy for the European qualifying examination (EQE) - decision by the Supervisory Board of the EQE

The retention periods for different types of documents are determined by consideration of the operational, legal and contractual requirements, and in line with best practice. The periods are counted from the final decision or latest action.

The length of retention is based on good practice, proof of final award (i.e. requirements of Art.134 EPC fulfilled), avoid fraudulent behaviour and financial accountability.

Data subjects and categories of personal data

Employees

Contact Information	
Contact Details	Emergency Contact Details
Phone Numbers	Working email address
Building area and site	
Building area and site	
Professional Experience & Affiliations	
CV	Qualifications Certifications
Correspondence	
Chat content	
Employment Information	
Department name and/or number	Language preference (of communication)

Office Location	Personnel Number
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Nationality
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Government Identifiers	
Passport Number	

Externals

Health Data	
Mobility needs	
Sensory and Electronic Information	
Audio Information	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Biometric	
Facial Recognition	Voice Recognition
Professional Experience & Affiliations	
CV	Qualifications Certifications
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Online invigilation data	
Audio input	Webcam captures
Employment Information	

Company Entity	Department name and/or number
Job Title Role	Language preference (of communication)
Office Location	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	First Name
Full Name	Gender
Surname	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Government Identifiers	
National Identity Card Details	Passport Number

Recipient of the personal data

Recipients of the data The Supervisory Board, the Examination Board, Examination Committees and an Examination Secretariat have access to the data of candidates to the extent needed to perform their respective duties as defined in the REE.

Depending on the EQE body, access to the data is granted on a need-to-know basis to EPO and non-EPO staff.

According to Article 23 REE: subject to Articles 21(2) and 22 REE, the members and deputy members of the Supervisory Board and the members of the Examination Board, the Examination Committees and the Secretariat shall be bound to secrecy both during and after their term of office with regard to all matters concerning the preparation of examination papers, the candidates and any relevant deliberations.
The personal data is disclosed, on a need-to-know basis, to the following recipients:
• the EPO's staff members of the Examination Secretariat;
• members of the Examination Committees and the Examination Board;
• EPO authorised users (`master` users);
• Administrators of the WISEflow platform at UNIWise and its subprocessors (management of ticketing of incidents and to the following data of the candidates and the members of the Examination Committees for the bidirectional communication channel (chats) during the examination; hosting services);BIT
• Finance departments for the fee processing
• Disciplinary Board of Appeal

Purpose of sharing For the purpose of organising and conducting the examination.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) Data Protection EU Comm Standard Contractual Clauses

Country where data might be transferred - Processor (Vendors) UNIwise - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Service provider's sub-processor is based in a third country

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal

data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., To mitigate the risk of a conflict of interest within the EPO (EPO employees may sit the examination) access to data is restricted to a very limited group of persons. Technical means protect the violation of confidentiality as far as possible, even from system administrators. Technical staff of the service providers who cannot be exempted from access are individually known and bound by a confidentiality declaration. All personal data are stored in secure IT applications according to the security standards of the EPO. External providers are under strict contractual obligation as defined by Procurement and BIT standards. Limited access to data is given to technical staff of the provider on an event driven basis for the purpose of system administration and error analysis. For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. Except for a specific purpose defined in advance by the DPS, only the minimum necessary data are shared with other external parties. These parties have systems which are in conformity with the EPO security standards and have implemented the appropriate technical and organisational measures in this respect. All EQE members are bound by secrecy under Article 23 REE. Access to these data is protected by the personal user accounts of the EB members. Marking of the answers is anonymous. Financial procedures for the administration of fee payment are executed by the EPO Finance department and their service providers.

Data protection statement

Data Protection Statement link internet
https://documents.epo.org/projects/babylon/epone t.nsf/0/83BF68AC46F67CEDC12588610031D23D/$F ile/data_protection_statement_on_the_processing_ of_personal_data_in_context_of_european_qualifyi ng_examination_en.pdf

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 225

Name Staff requests that require medical assessments by the EPO Health Services

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 423 - HR Essential Services

Entity Name - Processor (Entities) DG4 - 422 - HR Customer Engagement, DG4 - 46 - CIO / BIT

External processors

SAP

External processors	
Name SAP	

Microsoft

External processors	
Name Microsoft, Microsoft	

Cigna

External processors	
Name Cigna	

Description of the processing

Description This record refers to the medical assessments carried out by the EPO Occupational Health Services (OHS) upon request of the staff and in the cases provided for by the Service

Regulations.

The staff of the OHS consists of medical, para-medical and administrative staff.

The medical staff provide medical assessments in the following cases:
a. Assessment of dependants' disabilities or serious illness for the granting of special allowances and reimbursement:

Staff members can request via a MyFIPS online form the assessment of the medical conditions of their dependants for the granting of the allowances under Article 69(5)(8) and the reimbursements under Article 69(10) ServRegs. The request is received by the OHS staff and is stored in the EPO medical database (Cority).

The conclusion of the medical assessment (that do not contain any medical information) is sent to the requester and HR Salary Department for registration of the relevant information in FIPS and for payment purposes.

If the request is sent via the HR ticketing system, the HR Interlocutors will also have access to the administrative information of the request, but not to any medical information.

Outlook may also be used for sharing information between the OHS and the requester. If the OHS have to share any confidential medical information with the requester, the file containing such information will be encrypted or password protected.

Relevant legal provisions: Article 69(5)(8)(10), Article 89-90 ServRegs

b. Assessment of family member's illness for the granting of special and family leaves

Staff members send their requests to the HR Interlocutors via the HR ticketing system and per email they send the required medical information to the OHS.

Any medical information is stored by the OHS in the medical database.

The conclusion of the medical assessment (that do not contain any medical information) is sent to the HR Interlocutors via email for registration of the relevant information in FIPS. HR Interlocutors will also inform the requester and their line manager on the conclusions of the medical assessment (which does not contain any medical information).

Relevant legal provisions: Article 45b(1) ServRegs, Circ. 22 Rule 3 Article 45b(c)(ii)(iii) ServRegs, Article 59(3) ServRegs, Circ. 22 Rule 8 Article 59 ServRegs

c. Settlement of disputes between staff and the health insurance administrator (Cigna) on reimbursement of medical expenses
Staff members send their request normally via MyFIPS online form or email to the OHS. The

medical information provided is stored by the OHS in the medical database.

Exchange of information via email for the settlement of the disputes between Cigna and the OHS is possible and is encrypted via TSL (transport layer security). The conclusion of the medical assessment is sent to the requester and Cigna via email and, in principle, does not contain medical information.

Exchange of medical information of the requester among the EPO and Cigna medical staff and the requester's treating physician(s) is bases on the explicit consent expressed in the MyFIPS online form.

In some specific cases and in order to prevent any reimbursement disputes, Cigna may ask OHS for advice on the eligibility for reimbursement of a medical treatment. In these cases, the medical documents are, in principle, anonymized.

Relevant legal provisions: Circ. 236, Circ. 178, Article 89-90 ServRegs

c. Grant sick leave for spa cures

The request for a spa cure (A or B type) is sent by the staff member via MyFIPS online form to the OHS.

Family members and pensioners send requests for cures of type A per email to OHS. The request contains a medical prescription and report. The medical assessment of the OHS medical staff on the granting of the sick leaves is based on the said document.

The assessment is sent via email to the HR Interlocutors for the registration of the sick leaves in the HR database (SAP-FIPS), to the line manager and for cure of type A also to Cigna. This assessment does not contain any medical information.

The communication via email between Cigna and the OHS is encrypted via TSL (transport layer security). Exchange of medical information of the requester among the EPO and Cigna medical staff and the requester's treating physician(s) is bases on the explicit consent expressed in the MyFIPS online form.

Family members and pensioners send requests for cures of type B per email to Cigna directly.

Relevant legal provisions: Art 83 ServRegs , Circ. 367 Article. 1D Sick leave in case of spa cures, Circ. 368 Guide to Cover

In all the cases mentioned above:
•There is no exchange of medical information between the OHS staff and the management, the HRBP and the HR Interlocutors.
•Any medical information (e.g. date of the consultation, medical notes, medical reports) is stored in the EPO medical database (Cority)

Purpose of Processing Processing of medical data is necessary to • process the staff request for the granting of the benefits or the settlement of disputes as provided for in the Service Regulations • improve the wellbeing of staff and their family

Data subjects are:
•Employees
•Pensioners (for a. ,c., d. case)
•External (Employees' and pensioners' family members (for the d. cases), widow, heirs (for the a., c., d. cases), treating physicians of the requester)

In all the above-mentioned procedures, the following categories of personal data may be processed:

Surname, forename, gender, personnel number, date and place of birth, nationality, civil status, children's name and date of birth, languages, postal addresses, e-mail address, telephone numbers, room number, name, contact details of the treating physician, job profile, type of contract, line manager name, type and duration of absences from work, date/time of medical consultations, sickness statistics, sick leave certificates, medical opinions (always issued without medical data).

In all the above-mentioned procedures, the following special categories of personal data may be processed.

Medical data: personal medical history, medical reports provided by the staff member, medical reports provided by EPO specialists after a consultation with the employee, medical notes recorded after a consultation, medical certificates, diagnoses.

Data Retention Cority is used since 2006 as main medical database. As of 2016, data are stored only electronically in the EPO medical data base.

Currently, the data is kept in the electronic database permanently due to technical constraints.

However, by 2023 the following retention periods should be implemented:
a. Assessment of dependants' disabilities or serious illness for the granting of special allowances and reimbursement - 5 years as of the end date of the allowance.
b. Assessment of family member's illness for the granting of special and family leaves - 5 years as of the case closure date.
c. Settlement of disputes between staff and the health insurance administrator (Cigna) on reimbursement of medical expenses - 10 years as of the case closure date.
d. Grant sick leave for spa cures - 10 years as of the case closure date.

The retention periods apply unless a litigation is pending. In case of pending litigation, the retention period will be suspended until all means of redress have been exhausted or the decision has become final.

All data stored in the Outlook common boxes and calendars of the EPO OHS older than 5 years is deleted.

Personal data stored in SAP-FIPS have currently no retention period.

SAP-MyFIPS is used by the employees to send requests for cure, which are encryption protected. The encrypted data is automatically deleted from the server after 90 days and from the PC of the administrative staff when they confirm that the data has been uploaded to Cority or on closing the encryption application (MedXfer).

In principle all data are stored only electronically. However, there are still old medical paper files stored in secured locked rooms only accessible to authorised staff that should be deleted by 2022.

Data subjects and categories of personal data

Employees

General	
Personal Information in SAP	Special Categories of Data in SAP
Ticketing	
Ticket related data	
Health Data	

Health Data	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Personal Email	Phone Numbers
Working email address	
Correspondence	
Personal information provided voluntarily	
Family Information	
Children's Names	Child's birthday
Spouse's name	
Financial	
Bank Account Information	
Employment Information	
Contract Type	End Date
Grade	Hours of Work
Job Group	Job Title Role
Language preference (of communication)	Personnel Number
Room Number	
Personal Identification	
Age	Date of Birth
Full Name	Marital Status

Externals

Health Data	
Health Data	
Contact Information	
Contact Details	Home Address
Phone Numbers	

Financial	
Bank Account Information	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	Full Name

Former Employees

Ticketing	
Ticket related data	
Health Data	
Health Data	
Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers
Family Information	
Children's Names	Spouse's name
Financial	
Bank Account Information	
Employment Information	
End Date	
Personal Identification	
Age	Date of Birth
Disability or Specific Condition	Full Name
Marital Status	

Recipient of the personal data

Recipients of the data The following recipients may have access to the categories of personal data (excluding medical data) mentioned under points 1.2 and 1.17 on a need-to-know basis only:

•HR Interlocutors – in particular they are the ones that may receive the request (in the a., b. cases) and process it once they receive the medical conclusion (in the b. cases)
•Line manager–is informed by the HR Interlocutors when the b. requests are granted and by the OHS when d. requests are granted
•Legal Services may have access to personal data for the prevention and management of grievances
•Directorate Ethics and Compliance (DEC) may have access to personal data in the framework of their investigative mandate
•SAP–Centre of Excellence department – a very limited number of staff of this department provides technical support for the maintenance of the medical database (Cority), in particular for system configuration purposes (i.e. creation, update and deletion of general system settings including language; screen layouts including the configuration of fields displayed on screens; look-up tables; business rules including field input checks; roles and profiles) and users management (i.e. creation and deletion of user accounts and the assignment of roles)
•Microsoft Office
•SAP-FIPS

The following recipients may have access also to the medical data mentioned under point 1.2 and 1.17 on a need-to-know basis only:
•Treating physician of an employee – when the employee has expressly authorised the EPO medical staff to exchange information with their treating physician (according to Art. 89(3) ServRegs.
•Health insurance administrator (Cigna) – in the framework of processing cure requests, disputes on medical reimbursements, detecting health care frauds
•SAP–Centre of Excellence department – only one employee of this department with the role of system configurator is allowed to have full access also to medical data. This is a necessary requirement to ensure the functionality and efficiency of the application.

The data are not used for any other purposes nor disclosed to any other recipient.

Purpose of sharing

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Cigna - United Kingdom, Cigna - Switzerland, Microsoft - United States, SAP - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures The email exchange between the OHS and Cigna is secured via TLS (Transport Layer Security) which is intended to allow two email systems that normally communicate via SMTP (SMTP operates with no encryption) to establish a virtual encrypted “tunnel.” Once established, all of the communications between the two companies will pass through this tunnel, with the expectation that the information will be automatically encrypted., EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., Link to the Matrix of the access rights (https://epocloud-my.sharepoint.com/personal/mrossi_epo_org/Documents/Data%20Protection/DP%20Register/HR%20customer%20engagement/Medical%20files/old/Matrix%20of%20Cority%20access%20rights.docx?web=1), SAP-MyFIPS is used by the employees to send requests for cure, for special dependants’ allowances, settlements of medical reimbursement disputes which are encryption protected., Once a year (in Q1) a roles review and logs security audit is carried out. The user manager in SAP–Centre of Excellence department sends to the chief physicians of the EPO Health Services the list of users and their respective roles assigned to Cority. The chief physicians must verify and validate the list and roles. The logs security audit is done by the chief physicians directly, each one for the data they are

responsible for., Administrative staff of the EPO Health Services, HR Interlocutors, HR Officers and the system configurator of the SAP-Centre of Excellence department are required to sign a confidentiality and data protection declaration, Medical reports are sent via email to the staff member after being encrypted or password protected in accordance with the Office's recommendations (Outlook Migration to the Cloud- http://my.internal.epo.org/portal/private/epo/organisation/dg1/?WCM_GLOBAL_CONTEXT=/epo/intranet/organisation/dg1/vp1_org/announcements/2021/1612436889418_outlook_encripted_documents), When face-to-face consultations are not possible or the staff member prefers to have remote consultations, MS Teams is the application used in these cases. Staff is informed not to share messages or documents containing sensitive information during MS Teams (video)calls in accordance with the Office's recommendations (Using Microsoft Cloud tools- http://my.internal.epo.org/portal/private/epo/work/news/?WCM_GLOBAL_CONTEXT=/epo/intranet/work/news/2020/1588753875455_using_cloud_based_tools)., The access to the medical data base is strictly given only to authorised persons, namely •the EPO medical and para-medical staff, •the administrative staff of the medical services, •the System Configurator of the SAP–Centre of Excellence department, •the Emergency User - In urgent cases it is essential that an emergency user exists, in order to intervene in cases of severe malfunction of the system (such as failure of the system, total authorisation blockage or process deadlock). Therefore the emergency user needs the complete Cority access rights. The emergency user has full authorisation allowing the execution of all system and application functions without any authorisation restrictions The access rights allow the above mentioned staff to process and consult only the data for which they are responsible

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 227

Name Identity Management through Okta

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

Entity Name - Processor (Entities)

External processors

Okta Inc

External processors	
Name Okta Inc, Okta Inc	

Description of the processing

Description The EPO uses Okta's cloud-based software as a service (SaaS) platform for the purpose of Identity and Access management.

The processing operation involves user authentication via Okta. The authentication is required as soon as a user attempts to log in to a secure area of EPO online services that is accessible with a smart card or with account credentials obtained for using those customer facing services, such as for example Central Fee Payment, New User Area, Online Filing, eLearning, Bulk data download.

Okta is used for the coarse grained access, whereas the context based role definition and assignment is taken care of in the individual applications or services.

Purpose of Processing Identity and Access Management for externals

Data Retention - Logs are retained for 90 days
- Accounts can be deleted in Okta on request - or in any case will be deleted when the contract with Okta ends.
- Accounts associated with EPOLine credentials are retained in line with EPOLine data retention. If user (customer) is removed in EPOLine due to reaching the specified retention period or upon data subject request, then it will also be automatically removed in Okta.

Data subjects and categories of personal data

Externals

Network/application Interaction Data	
Session details	Session metadata
Physical and/or Digital Identifiable Assets	
Digital Certificate	Smart Card Number
Contact Information	
Mobile Phone Number	Personal Email
Working email address	
Employment Information	
Language preference (of communication)	
Browsing Information	
Browser type	IP Address
Network Interaction History	
Personal Identification	
First Name	Surname
User Account Information	
Account Number	Account Password

Employees

Network/application Interaction Data	
Session metadata	
Contact Information	
Working email address	
Personal Identification	

First Name	Surname
User Account Information	
Account Password	User ID

Recipient of the personal data

Recipients of the data Internal:
Information Security dept 4623
External:
Okta Inc and their affiliates

Purpose of sharing Internal:
Information Security dept 4623: for managing the identities and related access rights
External:
Okta Inc and their affiliates: to provide the identity and access management services (SAAS)

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Okta Inc - Costa Rica, Okta Inc - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, To provide the identity and access management services

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., Okta maintains administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of our Data, including Personal Data, as set forth in the Trust & Compliance Documentation. Okta regularly monitors compliance with these safeguards, Okta has obtained certification under the Asia-Pacific Economic Cooperation scheme of Privacy Recognition for Processors and processes personal data accordingly.	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 229

Name Legal Affairs cooperation with CPVO - Joint Seminar

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities) DG0 - 02 - Communication

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description As part of the cooperation between the Office and the Community Plant Variety Office (CPVO), as agreed in an Administrative Arrangement between the EPO and CPVO, D521 organises and conducts bilateral virtual seminars involving representatives of both offices, in order to share knowledge and working practices on plant-related patents and plant variety rights.

For the purposes of organising these virtual seminars, personal data of the participants are processed.

Each meeting leads to opening of an electronic file in the case management system of the Directorate (CMS) under a specific Log number together with the name of the responsible officer to whom the organisation is assigned within the Directorate. Personal data are also processed in MS Outlook for correspondence purposes like sending invitations, distributing the agenda, etc.

In order to share knowledge and working practices on plant-related patents and plant variety rights.

A paper version of the file might also be printed.

The processing of the data will also serve possible follow-up actions after the meeting (like distribution of report).

Data Retention Personal data associated with the practical organisation of the EPO/CPVO seminar are kept as long as necessary for the organisation of seminars, usually yearly or at even longer intervals, in the context of the cooperation agreement. Contact details of participants indicated by CPVO for a given meeting are kept to facilitate the organisation of the next meeting until a person is no longer participating.

Personal data associated with the meeting file created in the case management system, including minutes and reports, are kept for he duration of the Administrative Arrangement and 20 years after that.

Purpose of Processing The CPVO seminars serve to implement the Administrative Arrangement and annual workplans with a view to streamlining international initiatives with impact on the Patent Grant Process (“PGP”), foster a holistic approach to IP training and awareness, further develop trust and collaboration between the two organisations.

Data subjects and categories of personal data

Employees

General	
Any other information	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information

Personal information provided voluntarily	
Employment Information	
Job Title Role	
Personal Identification	
Full Name	Gender

Externals

General	
Any other information	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Company Entity	Job Title Role
Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data - CPVO
- PD02, EPO Event Management
- D521 Staff members
- D522 Staff members
- The external providers

Purpose of sharing Personal data is shared only with recipients who are involved in the logistics of organising the meeting.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation Community Plant Variety Office (CPVO)

Country where data might be transferred - Processor (Vendors) Microsoft - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Transfer mechanism(s) The recipient provided appropriate safeguards, A derogation in accordance with Art. 10 DPR

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 230

Name Email usage

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 46 - CIO / BIT

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft	

Indra

External processors	
Name Indra	

Description of the processing

Description Processing of personal data occurs within the email and calendar flows from and to the mailboxes of EPO staff when using Microsoft Outlook and Exchange Online, as well as any service provider that has been assigned an EPO email address.

In addition Outlook also includes non-optional connected experiences which are designed to enable more effective creation, communication, and collaboration.

Data Retention • Email information as well as any personal address book implemented by the EPO email system user is stored as long as the user wishes to maintain the message and as long as the user has a contractual obligation with the EPO.
• Email messages voluntarily deleted by the user are retained for 90 days and then purged.
• The personal information included in the Global address book and a user's mailbox is stored as long as a user (e.g. employee, contractor) has a contractual obligation with EPO. Once a contract expires, information is retained for maximum 1 year and a half for the purposes of collection from the EPO or possible renewal. After this period, information is deleted.
• In the cases of a legal claim or an administrative investigation, be it a disciplinary or criminal offense, personal data could be stored longer than the time limits indicated above. In such cases, which are out of BIT PD4.6 delegated controllership, the retention of personal data is decided on a case-by-case basis by the corresponding Delegated Controller.

At all times during the term of EPO's subscription, EPO will have the ability to access, extract and delete the data stored in Outlook and Exchange Online.
• Microsoft will retain EPO Data that remains stored in the Online Services in a limited function account for 90 days after expiration or termination of EPO's subscription so that Customer may extract the data.
After the 90-day retention period ends, Microsoft will disable EPO's account and delete the EPO Data and Personal Data stored in Online Services within an additional 90 days, unless authorised under the agreement with Microsoft to retain such data.
• For Personal Data in connection with the applications, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon EPO's request, unless authorised under the agreement with EPO to retain such data.

Purpose of Processing To enable the communication of e-mail messages, attachments and calendar-related actions amongst EPO staff and externals via user clients and Application Program Interfaces (APIs). -To offer to EPO email system users an address book to retrieve EPO recipients' addresses, mailing lists and groups - To have a trail of emails for IT troubleshooting and cybersecurity purposes. -To have a retention mechanism enabling EPO email system users to restore email messages which they have accidentally recently deleted. -Eventual requests to process Email usage personal data for purposes other than those stated above are to comply with Article 7 Circular 382 Information Security Guidelines.

Data subjects and categories of personal data

Contractors

Network/application Interaction Data	
Session content	Session details
Session metadata	
Sensory and Electronic Information	
Presence Status	
Physical and/or Digital Identifiable Assets	
Digital Certificate	Operating System Version
Workstation's Hostname (Physical or Virtual)	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Office Location
Room Number	
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Cookie Information	IP Address
Network Interaction History	URL
Personal Identification	
Digital signature	First Name
Surname	
User Account Information	
Membership Permissions	Ownership Permissions

User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
System-, Application-, Security-related Server Logs	Transaction-related Details

Employees

Network/application Interaction Data	
Session content	Session details
Session metadata	
Sensory and Electronic Information	
Presence Status	
Physical and/or Digital Identifiable Assets	
Digital Certificate	Operating System Version
Videoconference Room/Equipment Identifier	Workstation's Hostname (Physical or Virtual)
Contact Information	
Contact Details	Mobile Phone Number
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Line Reporting Manager
Office Location	Room Number
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information

IP Address	Network Interaction History
URL	
Personal Identification	
Digital signature	First Name
Surname	
User Account Information	
Membership Permissions	Ownership Permissions
User ID	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
System-, Application-, Security-related Server Logs	Transaction-related Details

Externals

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Personal Email	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Browsing Information	
Browsing Date and Time	IP Address
Network Interaction History	
Personal Identification	
Digital signature	First Name
Surname	
System Logs	
File data (name, size and/or hash)	System-, Application-, Security-related Server Logs

Transaction-related Details	

Former Employees

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Contact Details	Mobile Phone Number
Personal Email	Phone Numbers
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Browsing Information	
Browsing Date and Time	IP Address
Network Interaction History	
Personal Identification	
First Name	Surname
System Logs	
File data (name, size and/or hash)	System-, Application-, Security-related Server Logs
Transaction-related Details	

Prospective Employees

Network/application Interaction Data	
Session content	Session details
Session metadata	
Contact Information	
Contact Details	Country
Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number

Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Browsing Information	
Browsing Date and Time	IP Address
Network Interaction History	
Personal Identification	
First Name	Surname
System Logs	
File data (name, size and/or hash)	System-, Application-, Security-related Server Logs
Transaction-related Details	

Recipient of the personal data

Recipients of the data All EPO email system users.

BIT PD4.6 (Delegated Controller), more precisely BIT PACE 4615 and BIT Security 4623

The external processors.

Purpose of sharing All EPO email system users will have access to the Address Book information.

In the processing of email traffic and for the management of Exchange server, the only recipients are BIT PD4.6 (Delegated Controller) and the external processors which are tasked with the operation, maintenance and delivery of Exchange service.

More precisely, BIT PACE 4615 processes the personal data for email system administration, operation and maintenance purposes; while the recipients in BIT Security 4623 for email cybersecurity purposes.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Protection against malware, login to Azure Active Directory, error analysis, load balancing, diagnostics data, connected experiences, and processing for Microsoft’s business operations

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures For personal data processed on systems not hosted on EPO premises, the providers processing the

personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. Any personal data in transit over public networks between the EPO and Microsoft, or between Microsoft data centres is encrypted by default. Personal data as part of any data that are provided to Microsoft by, or on behalf of, EPO through use of the Microsoft 365 services is encrypted at rest. Regarding the implementation of the encryption, Microsoft uses state of the art encryption technologies. Furthermore, Microsoft employs least privilege access mechanisms to control access to personal data which are part of data that are provided to Microsoft by EPO and role-based access controls are employed to ensure that access to such personal data required for service operations is for an appropriate purpose and approved with management oversight. For Microsoft 365 Applications any required access by Microsoft is for a limited time. Microsoft 365 applications implement and maintain multiple security measures for the protection of personal data as part of any data that are provided to Microsoft by EPO through use of the Microsoft 365 services, which encompass the following: organisation of information security (e.g., security ownership, security roles and responsibilities, risk management program), asset management (e.g. asset inventory and asset handling), human resources security (e.g. security training), physical and environmental security (e.g. physical access to facilities, physical access to components, protection from disruptions, component disposal), communications and operations management controls (e.g. operational policy, data recovery procedures, anti-malware controls, event logging), access control measures (e.g. access policy, access authorisation, least privilege, integrity and confidentiality, authentication, network design), information security incident management (e.g. incident response process, service monitoring) and business continuity management. Microsoft also implements and maintain appropriate technical and organisational measures for protection of any other personal data distinct from the one described above, which are described in Microsoft Security Policy. Microsoft 365 applications have been configured to preserve the confidentiality of the information by employing the measures listed above. In addition, anonymous access is not authorised. Any information you add to Microsoft 365, be it via chat, videoconference, or file sharing, will be available only to the specific users and groups indicated in section 4 above. Microsoft 365 applications are certified in several security standards, including ISO27001, ISO 27002, SOC1 Type II, SOC2 Type II and ISO27018 Code of Practice for Protecting Personal Data in the Cloud. Microsoft conducts annual audits of the security of the computers, computing environment, and physical data centres that it uses in processing of personal data. The audits are performed by independent, third-party auditors according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.

Personal data is stored in the EU according to the application configuration implemented by the EPO. It may, however, be made available to subprocessors in other countries, depending on the requirements for maintenance, support or operation of cloud-hosted services, and the availability of this expertise. If access is granted, it is always temporarily and only to the data required for the specific maintenance, support or operation procedure being carried out. The following safeguards are implemented: • In all transfers to third countries, Microsoft uses EU Standard Contract Clauses for data transfer with its sub-processors. • Microsoft requires subprocessors to join the Microsoft Supplier Security and Privacy Assurance Program. This programme is designed to standardise and strengthen data handling practices, and to ensure that supplier business processes and systems are consistent with those of Microsoft. EPO-specific measures relating to the Exchange Online and Outlook: • EPO credentials via modern authentication are required in order to access the email inbox. • Access from devices which are not jointed to EPO’s domain is subject to MFA. • Authentication and authorization based on roles. MFA is enforced to activate any roles. • Access reviews on existing roles; audit history.

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 232

Name Institutional issues and matters relating to the Legal division and the Unitary Patent Division - provision of legal advice

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities) DG4 - 44 - General Administration

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft, Microsoft	

OpenText

External processors	
Name OpenText	

Description of the processing

Description Within Legal Affairs, D 5.2.3 Institutional Affairs, Legal and Unitary Patent Division provides legal advice in matters of the

domain of expertise of the Directorate, often in the form of explanatory notes, legal opinions, internal notes, reports, drafts for legal texts, presentations, letters, speaking notes etc. (hereinafter “legal advice”).

Requests to this end are received from the hierarchy or other units of the Office, including concerning adequate response to requests for cooperation with:
- other International Organisations or
- competent authorities of the Contracting States or
- any other third party.

Requests are usually received at a generic email account of the Directorate (D523inst@epo.org; legaldivision@epo.org) or by the Director.

They lead to the opening of an electronic file in the case management system of the Directorate (CMS) under a specific file number together with the name of the requester and the employee(s) to whom the matter is assigned within the Directorate. Requests might also be stored in the Outlook accounts of the Directorate. A paper version of the file might also be opened.

Once assigned to a Directorate member, the matter and legal question is identified, assessed, and answered to the requester via e-mail, orally, in paper form or by giving access to the document on a shared drive.

The handling of matters in/by the Directorate might require the organisation and holding of phone calls, physical or virtual meetings. Language Services might be involved as necessary for translation or editing.

For certain matters, an external attorney at law will be involved to assist, who will act as a "controller" in relation to personal data possibly associated with a specific case. The choice of a law firm/its location will a.o. depend on the area of expertise required.

The relevant correspondence, drafts and final legal advice are saved in the CMS and email accounts of the Directorate, in the paper version if one was created and possibly in working files created by the employee dealing with the matter on storage places provided by the Office. For certain matters requiring consultation of other units or information and/or sign-off by hierarchy, relevant information and documents are shared via a specific document management system (CommonLog or OpenText).

Personal data associated with the handling of a given request can be transmitted or transferred, for example to private or public entities outside the EEA, or to international organisations, where necessary to achieve an adequate response to the request.

The active processing ends with the closure of the matter.

Purpose of Processing 3. This requires retaining previous legal advice for later reference to harmonise legal practice., 2. This encompasses ensuring proper collaboration, consultation, alignement and hierarchy's approval., 4. It is also necessary for planning and managing the activities of the directorate, including reporting and statistics., 1. The processing of personal data is necessary for providing legal advice on matters within the expertise of D 5.2.3, Institutional Affairs, Legal and Unitary Patent Division.

Archiving of documents after the end of the retention period, as provided in Article 14 DPR, is described in a dedicated record.

Legal opinions provided by external attorneys are kept separately in databases and storage places provided by the Office where are also kept documents concerning the work of the Directorate, such as minutes of meetings.

Data Retention After the closure of a matter, related files are kept for up to 20 years.

The retention period begins to run on 1 January of the year immediately following the date on which the file was closed. This approach might be revised once the available tools will allow for an automatic follow-up and handling of retention times.

Certain files/parts of the file (such as correspondence concerning relations and cooperation with Member States or International Organisation) with particular value are permanently preserved.

Data subjects and categories of personal data

Contractors

General	
Assessment and legal opinions	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Employment Information	
Assessment and legal opinions	Company Entity
Personal Identification	
First Name	Full Name
Surname	

Employees

General	
Assessment and legal opinions	
Contact Information	
Phone Numbers	Working email address
Employment Information	

Assessment and legal opinions	Business Unit Division
Personal Identification	
First Name	Full Name
Surname	

Externals

General	
Legal opinions and assessments	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Employment Information	
Company Entity	
Personal Identification	
First Name	Full Name
Surname	

Former Employees

General	
Legal opinions and assessments	
Contact Information	
Contact Details	
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data The requester is usually a recipient.

Further recipients might be as described below, on a need to know basis and depending on the subject-matter of the request.

Within the EPOrg:
- Other units
- Hierarchy
- Administrative Council
when information or consultation is necessary to achieve one of the above mentioned purposes.

When recipients are outside the EPO, it is usually in the following circumstances:
- Attorney at law
- Addressee of a letter of content (e.g.: ILO, Ministry contact points in Host States...)

Furthermore, processors listed in point 1.8 are recipients.

Purpose of sharing The requester: to provide the advice sought.

Within the EPO
- Other units for information or consultation
- Hierarchy for information or approval
- Administrative Council for submission of CA documents

Outside the EPO:
- Attorney at law for obtaining legal services
- Addressee of a letter of content for information
- Processors: for technical support.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation Occasionally to International Organisations, depending on the subject matter of a matter.

Transfer mechanism(s) The recipient provided appropriate safeguards, A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OpenText - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 233

Name Legal practitioners' list and its maintenance

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft, Microsoft	

ServiceNow

External processors	
Name ServiceNow	

Description of the processing

Description Legal practitioners may take over representation in proceedings established by the EPC in the same way as a professional representative registered on the list if they provide evidence that they fulfil the specific requirements as outlined in Article 134(8) EPC.

The Legal Division is responsible for the registration and deletion of legal practitioners in an internal database, based on the decision of the President of the European Patent Office dated 21 November 2013 concerning the responsibilities of the Legal Division, OJ EPO 2013, 600 and for entry in the European Patent Register, Rule 143(1)h EPC.
For his registration, the data subject must provide personal data like name, address, gender, accompanied by documents of proof/evidence of belonging to the bar.
Likewise, the deletion requires a request by the legal practitioner himself or others (e.g. dependants, bar association). For the processing of deletion, special documents are required depending on the grounds of the deletion. Such documents are e.g. a death certificate or bar association exclusion.
The processing of the aforementioned requests might necessitate the sharing of the data with other units within the EPO to address questions arising from the case at stake, e.g. of legal nature.
Besides, the Legal Division provides other units of the EPO with relevant information necessary to perform tasks associated with being registered as legal practitioner, e.g. to allow invitation to specific events, seminars, surveys etc. Other contact detail exports or statistics can be provided internally, on request.
In terms of workflows, the request for registration and any change of name, address or other details must be addressed to the responsible Legal Division. Documents are received by post, e-mail with attachment,
fax, filed in Madras (EPO internal electronic repository), Customer Service Management.

Data Retention For reasons of legal certainty, personal data is kept up to 99 years, starting from the first entry date on the list of legal practitioners.

Purpose of Processing 4. Preparation of statistics, 1. The processing of personal data is necessary for the setting up, maintenance and publication of the list of legal practitioners by the Office and providing up-to-date information to stakeholders as well as all associated actions to e.g. ensure a proper and efficient information flow and management of associated activities. This encompasses following elements:, 3. provide Office's units with information necessary to perform tasks associated with being listed as legal practitioners, 2. registration and deletion from the list of legal practitioners and use of this information by the Office for related actions taking place during the patent granting process including name publication in European Patent Register

Data subjects and categories of personal data

Externals

Ticketing	
Ticket related data	
Contact Information	
Contact Details	Phone Numbers

Working email address	
Professional Experience & Affiliations	
Professional Memberships	Qualifications Certifications
European Patent Register Data	
Address	Data provided by the data subjects
Correspondence	
Personal information provided voluntarily	
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of patent procedure related information and publications
Employment Information	
Business Unit Division	Company Entity
Job Title Role	Office Location
Personal Identification	
First Name	Full Name
Gender	Surname
Signature	

Employees

Ticketing	
Ticket related data	
Contact Information	
Phone Numbers	Working email address
Employment Information	
Business Unit Division	Job Title Role
Office Location	Personnel Number
Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data Different business units at the EPO will have access to the information stored on the contact details database:

• DG0, DG1, DG5
• Other involvements are possible, e.g. Board of Appeals on a need-to-know basis

Purpose of sharing • DG1 as needed for the patent grant procedure
• Other internal contact detail exports or statistics on request for DG0, DG1, DG5, on a need to know basis
• Other involvements are possible, e.g. Board of Appeals in case of an appeal

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States, ServiceNow - Australia, ServiceNow - United States, ServiceNow - India, ServiceNow - Japan, ServiceNow - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 234

Name User Consultation on Guidelines for Examination

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

Infotel Conseil SA

External processors	
Name Infotel Conseil SA	

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description In the course of the annual revision of the Guidelines for Examination, an online user consultation is conducted by the delegated controller/D521. For these online consultations, personal data of the participants are collected.

Participation in the user consultation happens on a voluntary basis. Users are informed via, inter alia, the EPO's Official Journal, webnews items and social media platforms about the launch of the user consultation for filing any comments to the recently revised Guidelines. The comments must be filed via a webform on the EPO website.

Personal data is received and seen by a restricted number of EPO employees in the delegated controller's directorates.

After three months, all contributions to the consultation are anonymised, removing the ability to identify an individual and therefore destroying the personal data.

Data Retention Personal data processed are stored for the period of time necessary to achieve the purpose for which they have been processed.

The personal data entailed in the user consultation will be deleted three months after the end of the consultation.

Purpose of Processing The user consultation serves to collect feedback on the Guidelines in force and suggestions for amendments, with a view to address and reflect the user‘s wishes and concerns in the practice of the Office. Personal data processed in this context permits relating individual comments, preference and wishes to specific users groups, thus allowing proper assessment of the relevance of the feedback.

Data subjects and categories of personal data

Externals

General	
Answers to surveys, assessments or quizzes	Any other information
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Job Title Role	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data Access to the data is limited to the processor and to a resctricted number of staff in the delegated controller's units.

Infotel (platform for the survey)

All further sharing of information on the user consultation is on anonymous basis, i.e. do not allow to identify the participants and their answers.

Purpose of sharing Sharing the contributions and personal data of contributors with restricted number of staff from the delegated controller's units allows individual contributions to be attributed to specific user groups, for the sake of a proper assessment of the relevance of the feedback.
Infotel have access to the data as they provide the platform that collects the data.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 235

Name Associations' lists maintenance

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft, Microsoft	

ServiceNow

External processors	
Name ServiceNow	

Description of the processing

Description Pursuant to Article 134(1) EPC representation of natural and legal persons in proceedings established by the EPC may only be undertaken by professional representatives whose names appear on a list maintained for this purpose of the EPO. Pursuant to Rule 152(11) EPC an authorisation of an association of representatives shall be deemed to be an authorisation of any representative who can provide evidence that he practises within that association. This legal fiction allows a party to authorise several representatives as an association instead of singly, provided this association is registered with the EPO.

The Legal Division of the EPO has sole responsibility for the registration and deletion of associations.

The requestor(s) must provide personal data like personal name, name and address of the association,
representative number and signature, entry or deletion dates (if these should deviate from the actual processing date of the EPO). The request is sent to the Legal Division, preferably using the dedicated EPO Forms, by post, e-mail and attachment, fax or are filed OLF options or via the Customer Service Management.

Other than the processing of registration, changes to or deletions of associations, the processing may also involve the sharing of data with other units within the EPO, as necessary to:
- address related questions arising in the patent grant process,
- perform tasks associated with being listed as member of an association, e.g. invitation to specific events, seminars, surveys etc. by the Academy,
- monitor developments in this area (e.g. statistics).

Data Retention For reasons of legal certainty, personal data is kept up to 99 years, starting from the deletion date of the association.

Purpose of Processing 3- Preparation of statistics, 2– registration, administration and deletion of associations and associated respective entries in the European Patent Register., 1. The processing of personal data is necessary for the registration, administration and deletions of associations by the EPO and providing up-to-date information to competent units in the patent grant process toensure a proper and efficient information flow and management of associated activities.

Data subjects and categories of personal data

Externals

General	
Any other information	
Ticketing	
Ticket related data	
Contact Information	
Contact Details	

Professional Experience & Affiliations	
Professional Memberships	
Representation in EPO’s Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Supporting documentation	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Personal Identification	
First Name	Full Name
Surname	Signature

Employees

Ticketing	
Ticket related data	
Contact Information	
Phone Numbers	Working email address
Employment Information	
Business Unit Division	Job Title Role
Office Location	Personnel Number
Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data Different business units at the EPO will have access to the information stored on the contact details database:

• DG0, DG1, DG5
• Other involvements are possible, e.g. Board of Appeals on a need-to-know basis

Purpose of sharing • DG1 as needed for the patent grant procedure
• Other internal contact detail exports or statistics on request for DG0, DG1, DG5, on a need to know basis
• Other involvements are possible, e.g. Board of Appeals in case of an appeal

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States, ServiceNow - Australia, ServiceNow - United States, ServiceNow - India, ServiceNow - Japan, ServiceNow - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 239

Name Dispute settlement activities in national proceedings or arbitration context

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities) DG4 - 44 - General Administration

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft	

OpenText

External processors	
Name OpenText	

Arbitration tribunal

External processors

Name

Arbitration tribunal

Description of the processing

Description PD52 Legal Affairs is responsible for providing legal support in all kinds of domestic legal proceedings brought against the European Patent Organisation (EPOrg), and where the EPOrg is a party to arbitration proceedings. A dispute may be submitted to arbitration for example on the basis of an arbitration clause in a contract or following an ad hoc offer made by the EPOrg. Such alternative resolution is also offered to external data subjects in the situation envisaged in Art. 52 of the Data Protection Rules (DPR) (data protection arbitration).

To serve this purpose, personal data are processed at various stages of handling a case, of mainly the parties, their representatives, other participants in the proceedings in any capacity (such as experts, witnesses, bailiffs, judges...) or about third parties if for example their data are contained in the parties' submissions. Typically the data categories concerned in the course of handling a case include such data allowing identification and contact details of the persons above, as well as further information as necessary for providing legal support in the case (depending on the subject matter of the proceedings). The data are usually obtained from the exchange of submissions in a case, possibly also from internal fact-finding exercise/gathering of evidence or publicly available sources (e.g. internet, press).

The various stages will differ depending on the case and type of proceedings at stake. Typically involved operations on personal data upon handling a case are described below.

- For domestic legal proceedings:
A writ of summons is served by a bailiff or by letter. The Office’s unit having received it, generally the President’s office, forwards it to Legal Affairs.

- For arbitration proceedings:
Legal Affairs is involved from the formation of the arbitral tribunal.
For the specific case of data protection arbitration, a request is made through an online form to the President of the Office, who forwards the request to the DPO, who then forwards the request to Legal Affairs. The request is sent to the Permanent Court of Arbitration acting as appointing authority for the appointment of an arbitrator.

- Upon opening of a case in Legal Affairs, the responsible lawyer(s) is assigned. An electronic case file is opened in the case management system of the directorate (CMS). In some cases a paper file might also be created.

- Legal Affairs assesses the claim and procedure at stake and advises the EPO’s hierarchy. This legal support is provided for example in the form of

Purpose of Processing - to manage the relationship with external attorneys and to monitor billing, - to ensure statistical monitoring of disputes, - to defend and represent the EPOrg in domestic legal proceedings or arbitration proceedings, including the availability of dispute files for later reference.

explanatory notes, legal opinions, drafting submissions, emails and letters. This might require exchanging information with the hierarchy, the Administrative Council and/or other departments in the EPO, and/or with external law firms.

- The EPOrg is represented in the proceedings directly by Legal Affairs and/or by external law firms.

- Personal data are disclosed outside the Office as necessary for the conduct of the legal proceedings or arbitration (such as for the exchange of correspondence and submissions with opposing parties, with representatives, with national bodies or arbitral tribunal before which proceedings are pending).

- Correspondence and documents are stored in the CMS and email accounts of the directorate, in the paper file if one was created and possibly in electronic working files created by the employee dealing with the matter on storage places provided by the Office. As necessary for information, consultation or approval, documents or information related to a case are shared within the EPO using the usual internet channels such as Outlook, CommonLog, SharePoint and OneDrive Shared Drives.

- At the end of the procedure, Legal Affairs is involved in the implementation of measures to be taken to implement a court order or arbitral award, e.g. for payment of damages necessary data would be shared with relevant units to proceed with a payment.

- Once the last actions related to a case have been taken, the corresponding file(s) is closed and assigned an archive reference.

Archiving of documents after the end of the retention period, as provided in Article 14 DPR, is described in a dedicated record.

Data Retention After the closure of a matter, related files are kept for 20 years.

The retention period begins to run on 1 January of the year immediately following the date on which the file was closed. This approach might be revised once the available tools will allow for an automatic follow-up and handling of retention times.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	
Correspondence	

Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Personal Identification	
First Name	Full Name
Surname	Nationality
Signature	

Employees

Contact Information	
Phone Numbers	Working email address
Employment Information	
Department name and/or number	
Personal Identification	
First Name	Full Name
Surname	

Recipient of the personal data

Recipients of the data Within the EPO:
- Hierarchy
- Other EPO units (e.g. Employment Law, Language Services)

When recipients are outside the EPO, it is usually in the following circumstances:
- Judicial body or other body before which proceedings are pending
- Arbitral tribunal
- Parties to the proceedings
- Representatives

Purpose of sharing Within the EPO:
- Hierarchy / for information and/or approval
- Other EPO units e.g. Contract Law or Employment Law / for consultation; Language Services / for editing or translation requests

Outside the EPO:
- Judicial body or other body before which proceedings are pending / for the conduct of proceedings
- Arbitral tribunal / for appointment of an arbitrator (Permanent Court of Arbitration) or for the conduct of proceedings
- Parties to the proceedings / for the conduct of proceedings
- Representatives / for the conduct of proceedings

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation For domestic legal proceedings: any body having jurisdiction in the case at hand.
For data protection arbitration: Permanent Court of Arbitration (for appointment of arbitrator).

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OpenText - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Public Authorities/Government Bodies, Service provider, Conduct of proceedings

Transfer mechanism(s) The recipient provided appropriate safeguards, A derogation in accordance with Art. 10 DPR

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states, The data transfer is necessary for the establishment, exercise or defence of legal claims and their transmission is not precluded by agreements under international law or other applicable legal provisions of the European Patent Organisation

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 241

Name Central Fee Payment

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 41 - Finance

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 46 - CIO / BIT

External processors

SAP

External processors	
Name SAP	

Financial Institutions

External processors	
Name Financial Institutions	

Ingenico

External processors	
Name Ingenico	

Description of the processing

Description Personal data is processed to enable the patent applicants, representatives and other parties to pay patent fees and claim refunds.

To use Central Fee Payment, you need to:
1) either register with an email address and a password for paying via credit card or using the bank transfer functionality or
2) directly sign in with the smart card, if you wish to pay with your deposit account. In this case the smartcard needs to be linked to your deposit account and have necessary access rights (pay fees online, view fees online or plan fees online). Smart card access rights are the same as in epoline and they are managed in epoline .

Contact information details are entered when you register to the service with an email address and a password, by filling the registration form. Only the fields marked with an asterisk are compulsory.

Once you have accessed the service, you can select the application and fees you would like to pay and add them to the shopping cart. At checkout, the fees are validated by the service. Afterwards, you can select the payment method: bank transfer, credit card or deposit account (deposit account only if logged-in with smart card).

Processing
EPO: from EPO side the payment process is automated.
Customer: Smart card users: the process is manual when they create their user profile for the first time. They choose fee for payment manually.
Non smart card users: the process is manual when they create their user profile for the first time. After registration the sign-in is with e-mail and password.

Data Retention If considered appropriate personal data can also be deleted if it can reasonably be expected that there is not operational need anymore. At a maximum 10 years.

Purpose of Processing Enable patent applicants/representatives and other parties to pay patent fees and order and pay patent information products

Data subjects and categories of personal data

Externals

Applications' Log	
SAP Logs	
Contact Information	
Contact Details	Country
Home Address	Phone Numbers
Working email address	

Device Management Data	
Account ID	
Financial	
Bank Account Information	Bank Account Number
Credit Card Number	Debit Card Number
Deposit Account	
Browsing Information	
Cookie Information	
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data European Patent Office: PD4.1.2 Revenue Controls

Outside EPO: Registered users have access to their own data

Purpose of sharing Enabling of online fee payment

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Ingenico - Unknown, SAP - United States

Reasons for the transfer Financial Institution's intervention is necessary for the good performance of the Contract .

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet
https://documents.epo.org/projects/babylon/eponet.nsf/0/83BF68AC46F67CEDC12588610031D23D/$File/data_protection_statement_on_the_processing_of_personal_data_within_framework_of_central_fee_payment_service_en.pdf

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 244

Name European, international and PCT related legal advice (D 5.2.2)

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft, Microsoft	

OpenText

External processors	
Name OpenText	

Description of the processing

Description D 5.2.2 receives requests from the hierarchy, other units of the Office or external parties seeking advice in matters of the domain of expertise of the Directorate (i.e. European, International and PCT related), to be provided in the form of explanatory notes, legal opinions, internal notes, reports, drafts for legal texts, presentations, letters, speaking notes etc. (hereinafter “legal advice”). This includes requests and processing of personal data to cooperate with:
- other Organs of the European Patent Organisation (Administrative Council),
- other International Organisations or
- competent authorities of the Contracting States

Requests are usually received at a generic email account of the Directorate or by the Director. They lead to the opening of an electronic file in the case management system of the Directorate (CMS) under a specific Log number together with the name of the requester and the case handler to whom the case is assigned within the Directorate. Requests might also be stored in the outlook accounts of the directorate (generic email account). A paper version of the file might also be printed.

Once assigned to a team member, the matter and legal question is identified, assessed, and answered to the requester via e-mail, orally, in paper form or by giving access to the document on a shared drive. The handling of matters in/by the Directorate might also require the organisation and holding of phone calls, physical or virtual meetings. D522 might involve an attorney at law. The relevant correspondence, drafts and final legal advice are saved in the CMS and, the case be, in a generic email account of the directorate.

The active processing ends with the closure of the case.

Data Retention Personal data for non patent-file related matters is kept for the default retention time period for legal advice of Legal Affairs (provided in the Mattersphere Case Management System record) except for cases where e. g. President, Vice President or other high ranked Officers were involved in order to be able to document the decision-making process.

Personal data in patent-file related matters (European patent applications and European patents) should be kept for thirty years to cover the longest possible period under Rule 147 EPC.

The said retention periods will be applied as follows: When a file having reached the end of the retention period is consulted by a staff member, it will be anonymised or destroyed. This approach will be revised once the available tools will allow for an automatic follow-up and handling of retention times.

Purpose of Processing The processing of personal data is necessary for providing advice on matters within the expertise of 522. This encompasses: (i) Questions of legal nature, (ii) advising and supporting on confidential deliberations and decision-making of the Office, (iii) provide up-to-date information to stakeholders as well as taking associated actions to e. g. ensure a proper and efficient information flow and management of associated activities, (iv) promoting the legal framework of the Organisation, also through awareness raising, (v) Handling with requests outside the direct expertise, if requested by senior management, (vi) planning and managing the activities of the directorate, including statistics, (vii) enabling the availability of previous advice for later reference in the event of subsequent related request or litigation, and (viii) archiving and statistical purposes.

Data subjects and categories of personal data

Employees

General	
Any other information	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Business Unit Division	
Personal Identification	
Full Name	

Externals

General	
Any other information	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Company Entity	Job Title Role
Office Location	
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data - The requestor
- PD52 Hierarchy
- Other units or external parties
- The external processors

Purpose of sharing Data is shared with the requestor in order to deliver the legal advice requested.

Data is shared with hierarchy and other units when information or consultation is necessary to achieve one of the above mentioned purposes.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Adequacy Decision

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OpenText - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 246

Name Archives Legal Affairs

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Description of the processing

Description Since the inception of the EPO, Legal Affairs has been responsible for the archiving of documents of historical, institutional and/or legal relevance to the EPO.

This record covers the processing operations of personal data related to this archiving*.

The personal data is archived in:
1) the paper based archive, where paper documents (including files) have been classified and stored in a separate room along a dedicated nomenclature. Legal Affairs' staff is granted access by the archivist, on a need-to-know basis.
2) the electronic archive, made of the electronic files and documents from Legal Affairs' Case Management System (CSM) which are being kept after the period of active work on the files (after closure of the matter). The files are stored separately for each directorate within Legal Affairs. Access is restricted to the staff of the corresponding directorate, on a need-to-know basis.

This approach will be revisited when the available tools will provide automated and differentiated means to e.g. identify, anonymize and/or pseudonymize the personal data.

*Archiving in the meaning of the DPR. It refers to the data kept after the elapsing of the retention period. For the storage of personal data until the elapsing of the retention period(s), it is referred to the relevant record(s) of processing operation.

Data Retention All processing operations under the responsibility of the delegated controller are described in the relevant records of processing operation, which state the applicable retention period(s). This archive record describes the way the personal data is kept/archived, should it not be destroyed at the end of the applicable retention period.

Purpose of Processing Archiving of documents of historical, institutional and/or legal relevance to the EPO.

Data subjects and categories of personal data

Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Thermal Information

Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Representation in EPO’s Patent Granting Process	
Representative registration number (ID)	
Telephony Interaction Data	
Telephony Session Content	Telephony Session Details
Telephony Session Metadata	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
General	
Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	Legal opinions and assessments

Nomination justificative	Personal Information in SAP
Sensitive Personal Data in SAP	Special Categories of Data in SAP
User association	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Home Leave Address	Mobile Phone Number
Personal Email	Phone Numbers
Previous Residence Address	Private Phone Number
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
Diagnostic tools’ results	IDP
Instructor related data	Learning external events
Learning history	Learning plan
Ratings	Social learning inputs
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	

Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Smart Card Number

Videoconference Room/Equipment Identifier	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Active/Inactive Indicator	Appeals Records Information
Assessment and legal opinions	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	Disciplinary Action
Duration of employment	End Date
End Date and Reason for Termination	EPO access badge number
Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Group
Job Title Role	Language preference (of communication)
Line Reporting Manager	Membership in a EPO Staff Committee
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Record of Maternity Leave	Rewards history

Room Number	Salary
Start Date	Weight
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Results on phishing attempts (entered credential not processed)	Session content
Session details	Session metadata
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Examination content data	
Examination marks	Examination result
Family Information	
Child’s Level/Year of Studies	Child’s School Enrolment Date Start
Children's Names	Child's birthday
Composition of the family (number of dependent children/persons)	Parents' Names
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number

Bank Statements	Bonus Payments
Compensation Data	Credit Card Number
Credit History	Debit Card Number
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Membership Permissions
Ownership Permissions	Password
Password Hash	Third-party User Identifier
User ID	
Government Identifiers	
Car registration documents	Driving Licence Number
National Identification Number	National Identity Card Details
Passport Number	Social Security Number

Externals

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Sensory and Electronic Information	

Audio Information	Electronic Information
Presence Status	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Representation in EPO’s Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Telephony Session Content	Telephony Session Details
Telephony Session Metadata	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	

Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Nomination justificative	User association
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Ratings
Social learning inputs	
European Patent Register Data	
Address	Data provided by the data subjects
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag

Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress

Operating System Version	Smart Card Number
Videoconference Room/Equipment Identifier	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Facial Recognition	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Employment Information	
Active/Inactive Indicator	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Duration of employment	End Date
EPO access badge number	Hours of Work
Job Title Role	Language preference (of communication)
Membership in a EPO Staff Committee	Office Location
Previous Work History	Record of Maternity Leave
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV

Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Examination content data	
Examination marks	Examination result
Financial	
Bank Account Information	Bank Account Number
Bank details	Credit Card Number
Debit Card Number	Fund Reservation Requests
Information on home loans	Insurance Information
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Membership Permissions
Ownership Permissions	Password Hash
Third-party User Identifier	User ID
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	

Recipient of the personal data

Recipients of the data - Employees of the delegated controller's units
- Other stakeholders

Purpose of sharing - Employees of the delegated controller's units: Access on a need to know-basis, i.e. when dealing with a matter in connection with the archived file concerned, requiring access to the archived file.
- Other stak: Depending on the particular circumstances of a case, it might be necessary to share information outside the delegated controller's unit.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 247

Name Mattersphere Case Management System in Legal Affairs/PD5.2

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Description of the processing

Description The delegated controller/Legal affairs uses the software "mattersphere", a case management, knowledge database, electronic storage and archiving system (hereinafter “CMS”) from Thomson Reuters.

Each Directorate within the delegated controller's unit has an own area in the CMS which is not accessible by other directorates within or outside Legal Affairs. Each directorate can open new cases (so-called log files or matters) which are used to assign working requests to members (case handlers) of the relevant teams, gather the relevant information, document the elaboration of inputs.

The log files entail mainly:
1) a page with key information on each case (so-called metadata) entered in pre-defined fields, such as subject matter, requester's name and contact details, case handler within the unit, line managers of case handler, unit concerned, matter type.
2) attachments (such as email exchanges, documents, drafts, legal opinions).

At the end of the applicable retention period, the relevant files are either destroyed (deleted), anonymised or archived (archiving activities are described in a separate record).

Data Retention The default retention period applicable for the personal data/documents entailed in the CMS is 20 years, unless a different retention period is mentioned in a specific record of processing operations of PD 5.2. Legal Affairs (the applicable data retention schemes depend on the type of personal data processed and the purpose of that processing).

The retention period usually begins to run on 1 January of the year immediately following the date on which the file was closed.

Purpose of Processing The purpose of the processing is electronic case- knowledge- storage- and archive management in Legal Affairs. This encompasses the need to: 1. ensure proper preparation of subsequent actions e.g. further communications, oral proceedings, final decision; 2. preparation of statistics and overview for reporting/statistical purposes 3. retrieval of previous advice as precedence, example and reference when dealing with new requests, and with a view to harmonise internal and external practice for archiving purposes (archiving is subject of a separate record).

Data subjects and categories of personal data

Employees

Matter/Log file	
Attachments	Metadata
General	
Any other information	
Ticketing	
Ticket related data	
Contact Information	
Contact Details	

Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	

Externals

Matter/Log file	
Attachments	Metadata
General	
Any other information	
Ticketing	
Ticket related data	
Contact Information	
Contact Details	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	

Recipient of the personal data

Recipients of the data The content of the CMS is only accessible to the staff of the relevant directorate, within the delegated controller's unit. If any sharing of information entailed in the CMS is necessary outside the delegated controller's unit, it is not done via providing access to the file in CMS.
Circumstances and ways of sharing depend on the different types of case/personal data processing and their purposes, as described in the records dedicated to the different types of processing.

Purpose of sharing Need to know.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors) TRE Thomson Reuters - Luxembourg

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 249

Name Personal data processing related to team and service quality management in the interpreting area

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 44 - General Administration

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 46 - CIO / BIT

External processors

Microsoft

External processors	
Name Microsoft	

Description of the processing

Description 1) The interpreting department doesn’t advertise any vacancies. It regularly receives spontaneous applications from freelance interpreters who would like to join the EPO interpreter pool. In principle, this pool is always open for new candidates and continually increased based on the needs of the moment. Candidates usually send an application letter or a CV by email to the EPO (Dept. 4.4.3.2 "Interpreting and Central Support"), i.e. to the generic Outlook Mailbox (Interpreting) or directly to HoD 4.4.3.2 or to the 4.4.3.2 staff member who is concerned with this process.

2) Applications from candidates who are not found to be suitably qualified are deleted immediately after they were informed about this.
Candidates who are found to be suitably qualified are then asked to send their CVs (if missing) and degree certificates and this information until the need arises and for max. 5 years (waiting list); for non-EPO languages data is kept for 10 years because the need arises only very rarely.

3) The so collected data are then stored in a dedicated and access-restricted folder on the W-Drive and are entered into IAS (Interpreter Administration System), the personal data relevant for receiving a Password/User ID are sent to User Registration (form to be filled in) and the relevant personal data for accessing the dedicated MS Teams page (email address) are entered into MS Teams

For ensuring the required quality of the delivered interpreting services, evaluation reports are drawn up on a regular basis. These data are stored in a dedicated and access-restricted folder on SharePoint.

4) application documents, CVs and degree certificates are kept for a maximum of 5 years if candidates have been found to be suitably qualified.

Processing is partly automated.

*Art. 10 of the "Conditions of employment for interpreters at the European Patent Office", Codex, Part 2f.

Data Retention Application documents, CVs and degree certificates are directly deleted after examination of the application or, in the case of sufficiently qualified candidates, are kept for max. 5 years. For non-EPO languages, these personal data are kept for 10 years.

Personal data of interpreters who are working for the EPO or have started doing so are kept for the duration of the employment relation with the EPO

Interpreter contracts and declarations regarding social security status (on paper until 2019) have to be kept for additional 10 years.

Purpose of Processing The personal data of interpreters employed at the EPO on short-term contracts are processed for the purpose of providing the EPO with the services of interpreters of the highest standard of ability, efficiency and integrity (cf. Art. 1,2 and 3 of the "Conditions of employment for interpreters at the European Patent Office", Codex, Part 2f). The processing of personal data is necessary for: - keeping a pool of accredited and appropriately qualified interpreters; - quality management purposes (induction of newly selected candidates and ensuring service quality) - administering the payment process Legal basis: Art. 14 (1), 31 EPC Article 14 EPC: "Languages of the European Patent Office, European patent applications and other documents" Article 31 EPC: "Languages of the Administrative Council" Conditions of employment for interpreters at the European Patent Office", Codex, Part 2f

Data subjects and categories of personal data

Externals

General	
Any other information	
Contact Information	
Contact Details	Phone Numbers
Working email address	
Professional Experience & Affiliations	
CV	
Correspondence	
Any other information	
Travel & Expense	
Expense Details	
Employment Information	
Previous Work History	
Personal Identification	
Age	Date of Birth
Full Name	Nationality
Education & Skills	
Languages	

Recipient of the personal data

Recipients of the data The applications of interpreters are accessible to
- HoD 4.4.3.2
- the 4.4.3.2 staff member responsible for the process
- In case of applications coming in via the generic Outlook Mailbox Interpreting, the data is accessed by 4.4.3.2 staff members responsible for interpreter administration
= recipients within the controller (EPO) including individuals from different operational units.

EPO external technicians involved in the organisation of the oral proceedings, they get weekly overviews for the purpose of enabling the oral proceedings.

Certain types of personal data (name, address, monthly remuneration plus the relevant internal tax (i. e. gross and net of tax) are sent to national tax/financial authorities in the interpreters' countries of residence (see Art. 14 (2) of the Conditions of Employment for Interpreters at the EPO, Codex, Part 2f)).

The data categories mobile phone number and e-mail address are made accessible on a dedicated MS Teams Page (EPO Interpreters' Teams page) and are - depending on consent - shared with courier delivery services and law firms (for recommendation).

Purpose of sharing N/A

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, All personal data related to IAS are stored in secure IT applications according to the security standards of EPO. These include: • User authentication: internal access (by D443) is based on Windows authentication, with Single Sign On, based on active directory groups. External access by interpreters is made via IAS External. Access is done via either the JUNIPER portal (https://telework.epo.org/languageservice), where interpreters enter their Windows user name and password to login. Since 2021, IAS External has also been defined as an Azure application. Authentication is based on the Standard authentication method defined for all EPO Azure applications (Windows user account + password + Multiple-factor authentication); • Access control: IAS and IAS External have only two roles: internal users or interpreters. These roles are “hard-coded” in the application and managed by Active directory groups. Requesters are not defined in the application: any EPO user can access the public page of IAS External to submit a request for interpreters. • Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; • Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; • Security incidence response: 24/7 monitoring for incidents, on-call security expert.

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 250

Name Convergence of practice (SP2023 Programme 4.4.2)

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

Zoom

External processors	
Name Zoom	

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft, Microsoft	

OpenText

External processors

Name	
OpenText	

Description of the processing

Description As part of the SP2023, a Convergence of Practice Programme has been established to identify, reduce and overcome diverging practices before national patent offices and the EPO.
Each EPC Member State and extension states, the Institute of professional representatives (epi) and Business Europe are asked to submit a representative to participate in meetings and share opinions of the entity they are representing on discussed proposals. The details are collected by email and used to establish lists of participants. The list of participants, and any e-mails sent to the participants of the working group by the Chair will possibly be stored in Microsoft tools (e.g. outlook, window explorer) or in the Case Management System of Legal Affairs (CMS). The minutes and reports will include the abbreviations of the represented States and user organisations but no indication who represented the State.
The meetings are usually held virtually and include the nominated participants of the working group from the EPC contracting states, possibly extension states, user organisations (usually epi & BusinessEurope), and the representatives of the EPO (Lawyers from the delegated controller's unit and examiners from DG1).

Data Retention Personal data processed are stored for the period of time necessary to achieve the purpose for which they have been processed.

Purpose of Processing The co-operation programme on the convergence of practice aims at reducing or possibly overcoming these differences by setting best practices in identified areas where it could be expected that a more uniform approach would provide the most beneficial results for users and patent offices.
This implementation requires the identification of the individuals representing the States or associations which participate in the discussions organised by the EPO, setting up of corresponding lists, organisation and holding of meetings, sharing opinions on the document to be prepared etc. Personal data is processed: To identify participants, to facilitate the necessary exchanges of views between the stakeholders involved, to elaborate a common proposal to be adopted by the Administrative Council of the EPO, and to keep track of the elaboration process, for historical and legal certainty purposes

Data subjects and categories of personal data

Employees

General	
Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	
Contact Information	
Mobile Phone Number	Phone Numbers
Working email address	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	

Employment Information	
Assessment and legal opinions	Department name and/or number
Job Title Role	
Personal Identification	
Full Name	

Externals

General	
Any other information	Input provided during the deliberation and decision-making process
Legal opinions and assessments	User association
Ticketing	
Ticket related data	
Contact Information	
Contact Details	Working email address
Professional Experience & Affiliations	
CV	
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Business Unit Division	Company Entity
Personal Identification	
Full Name	

Recipient of the personal data

Recipients of the data The participants of the working group
Senior Management of the EPO
Other units of the EPO as necessary
External Contractors involved in providing a platform for the working group

Purpose of sharing The participants of the working group are informed of the list of participants to facilitate discussions between participants (including both internal EPO employees and external participants.
Senior management of the EPO and other units of the EPO are informed of the list of be aware of who is participating, participants to monitor developments in the meetings and any conclusions drawn.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation National Patent Offices of EPC Extension States

Transfer mechanism(s) The recipient provided appropriate safeguards, A derogation in accordance with Art. 10 DPR

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OpenText - United States, TRE Thomson Reuters - Luxembourg, Zoom - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Derogations Art. 10 DPR The transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or to perform obligations arising from its duty of co-operation with the contracting states

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 251

Name General Authorisations maintenance

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft, Microsoft	

ServiceNow

External processors	
Name ServiceNow	

Description of the processing

Description The representation in proceedings with the EPO may be undertaken by a person registered on the list of professional representatives before the EPO, legal practitioners (Article 134(8) EPC as well as, under specific conditions, by an employee of a party (Article 133(3) EPC).

Whereas legal practitioners and employees must always file an authorisation, professional representatives are only obliged to file an authorisation in specific cases (cf. Decision of the President of the European Patent Office dated 12 July 2007 on the filing of authorisations (OJ EPO 2007, Special edition No. 3, 128). To this end, all these representatives may be individually or generally authorised (cf. Rule 152(5) EPC). General authorisations are registered, administered and deleted by the Legal Division competent to this end (OJ EPO 2013, 600).

General Authorisations must be filed in the original and are received by post or electronically via permitted OLF (online filing).

For the registration of a general authorisation the requestor(s) must provide personal data like name and address of the authorisor(s) and authorisee(s) as well as position within the company (if applicable) of the signatory.

Specific documents might be required, such as certification of employment or commercial register extract.

In case of an employee under Article 133(3) EPC, the confirmation letter
is sent to the authorisor rather than the authorised employee. In all other cases,
the confirmation letter is sent to the representative with a copy of the newly registered GA or a copy of the updated GA.

The general authorisation, including the level of rights awarded, is registered in the EPO's internal database

Data Retention Personal data processed are stored for the period of time necessary to achieve the purpose for which they have been processed.

Should a GA (General Authorisation) be withdrawn, its status would become inactive in the system. The retention time is 99 years after the withdrawal.
When a function/mandate as authorisor or authorisee is withdrawn from a running GA, corresponding status of that data subject becomes inactive. Relevant personal data is destroyed when the GA reaches the end of its retention time.

A GA and related functions of authorisor or authorisee, together with related personal data, are destroyed at the latest 99 years after the last authorisee has been withdrawn from the list in which they were registered (e.g. as professional representative, legal practitioner etc).

Purpose of Processing Registration, deletion and administration of general authorisations as well as provision of up-to-date information to internal units to ensure a proper and efficient information flow and management of associated activities in the patent grant process as well as the preparation of statistics

Data subjects and categories of personal data

Externals

Ticketing	
Ticket related data	
Contact Information	
Contact Details	Country
Home Address	Phone Numbers
Working email address	
Representation in EPO’s Patent Granting Process	
Affiliation to Association of professional representatives	Authorisee function
Authorisor function	EPO CDS (Client Data System) categories related to the Representation role
Representative registration number (ID)	Role in the Patent Grant Procedure
Supporting documentation	
Employment Information	
Company Entity	Job Title Role
Personal Identification	
Full Name	Gender
Surname	Signature

Employees

Ticketing	
Ticket related data	
Contact Information	
Phone Numbers	Working email address
Employment Information	
Business Unit Division	Job Title Role
Office Location	Personnel Number
Personal Identification	

Full Name	Gender

Recipient of the personal data

Recipients of the data Different business units at the EPO will have access to the information stored on the contact details database:

• DG0, DG1, DG5
• Other involvements are possible, e.g. Board of Appeals on a need-to-know basis

Purpose of sharing • DG1 as needed for the patent if required in specific patent applications.
• Other internal contact detail exports or statistics on request for DG0, DG1, DG5, on a need to know basis
• Other involvements are possible, e.g. Board of Appeals in case of an appeal

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States, ServiceNow - Australia, ServiceNow - United States, ServiceNow - India, ServiceNow - Japan, ServiceNow - United Kingdom

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 252

Name Programme 4.5.3 “Improving the quality of PCT products and services”

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities) DG0 - 02 - Communication

External processors

Zoom

External processors	
Name Zoom	

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft, Microsoft	

OpenText

External processors

Name

OpenText

Description of the processing

Description Programme 4.5.3 aims at strengthening the attractiveness of the EPO in the context of the PCT by further improving the quality of its PCT products and services. This programme covers projects and tracked activities that require cooperation with WIPO, PCT Contracting States including IP5 Offices. It is designed to enable the EPO to stay in the lead of endeavors for a global convergence of requirements and/or practices via the PCT, while at the same time ensuring that the interests of the EPO, its users and stakeholders are fulfilled.

Personal data is processed where it is necessary for the performance of the projects and tracked activities under this programme:

Collected data is stored on a shared drive of Directorate D 5.2.2 or in the Case Management System of PD52 (CMS), or, as far as older data is concerned, in paper form. In most cases, the personal data collected are of professional nature, i.e. names, Organisation, professional e-mail addresses, professional titles/roles, department names, correspondence, substantive comments, contributions.

Other personal data may also be collected where necessary for the organisation of meetings (e.g. meetings with WIPO and PCT Contracting States, meetings between IP5 Offices).

Collected data may be shared outside the EPO either within the context of the PCT procedure or for cooperation activities. In this latter case, the recipients are usually WIPO or an IP Office of a PCT Contracting State which are involved in the activity/meeting within the context of which the data was collected. For some meetings, the list of participants annexed to the summary of discussions of that meeting is included in a document published on WIPO’s website.

In case of physical meetings, group pictures might be taken and be published on the EPO's intranet. The case be, further personal data might be processed, such as dietary habits or mobility needs.

Purpose of Processing Data is processed within the context of the PCT procedure or for cooperation activities related to the PCT.

Data Retention - The default retention period of 20 years of Legal Affairs will be applied as follows: When a file having reached the retention period of 20 years is consulted by a staff member, it will be assessed and decided whether the said file should continue to be kept as-is, anonymised or destroyed. Files considered still necessary will be kept 10 more years, after which the same procedure applies again until destruction or anonymisation.
This approach will be revised once the available tools will allow for an automatic follow-up of retention times.
- The minutes of meetings, entailing the name of the Chairperson, as well as the list of participants are kept without time limitation.
- Information on dietary habits or physical mobility is deleted as soon as is it not anymore necessary, usually within 3 months after the event.

Data subjects and categories of personal data

Externals

General	
Any other information	User association
Contact Information	
Country	Phone Numbers
Working email address	
Professional Experience & Affiliations	
Affiliation	Professional Memberships
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Business Unit Division	Company Entity
Department name and/or number	Job Title Role
Personal Identification	
Full Name	Gender

Employees

General

Any other information	Assessment and legal opinions
Input provided during the deliberation and decision-making process	
Ticketing	
Ticket related data	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Any other information	
Employment Information	
Assessment and legal opinions	Business Unit Division
Department name and/or number	Job Title Role
Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data Internal recipients: the EPO hierarchy and colleagues from other departments who are involved in projects/activities covered by Programme 4.5.3. External recipients: WIPO, IP Offices of PCT Contracting States , the external processors, and, in rare cases, external persons/the public

Purpose of sharing Information or cooperation purposes

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OpenText - United States, TRE Thomson Reuters - Luxembourg, Zoom - United States

Transfer to public authority and/or International Organisation WIPO and IP Offices of PCT Contracting States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, International cooperation activities

Transfer mechanism(s) The recipient provided appropriate safeguards, Adequacy Decision, Legally binding and enforceable instrument between public authorities or bodies

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 254

Name EPO Academy

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 51 - Cooperation and Patent Academy

Entity Name - Processor (Entities) DG0 - 02 - Communication, DG4 - 46 - CIO / BIT

External processors

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description A. Europen Patent Academy is responsible for keeping a database of email addresses used for a mailing list for informing data subjects about publications, activities and events and for sending newsletter and e-alerts based on self-subscription.
This personal data part of this database may be shared internally among EPO organisational units (e.g the EPO PD Communication) in order for them to contact data subjects in case of future meetings/events. The Academy stores email addresses for the distribution of the newsletter in a database operated by an external company.

B. European Patent Academy is responsible for the organisation of some events (such as, online and onsite courses, lectures, seminars, conferences, workshops).

These events may also be streamed live and recorded and the recordings used for promotional and educational purposes.
The audio-visual material produced may be published on the EPO internal (e.g. Intranet, e-

centre of the European Patent Academy or the internal EPO podcast page) and/or on external platforms (e.g. EPO website and podcast platforms) or social media (e.g YouTube, LinkedIn, Twitter, Facebook).

Although the EPO may use these social media channels to inform about and promote initiatives, this does not mean in any way that the EPO endorses them nor the way they process users' personal data.

During the events, if the audience is allowed to ask question (by using Slido or other applications as well as the chat/comment function on the channels of social media) the EPO will, when receiving your question, forward this question to the moderator, who in turn will inform the speaker/presenter with the mention of your first name only, without further personal information from the person asking the question, nor pictures or video from this person.Depending on the platform used, the attendees can choose to post their comment and/or opinions publicly or anonymously.

When data subjects register to events organised by the Academy, they can also indicate their interests for the mailing list.

For onsite events, EPO PD Communication organises the event contacting the speakers and all attendees in order to establish catering, dietary requirements and other preferences.

C. European Patent Academy is responsible for the organisation of research programmes and the selection process of appropriate candidates and their proposed research schemes. In case of successful selection of a candidate and the proposed research scheme, all personal data will form part of a respective agreement to be signed between the candidate and the EPO and the personal data processed will be used for sending communications about the research programme and further activities carried out by the European Patent Academy.

The Academy's didactics unit uses the Alfresco database. It is not used it to contact the public just to store and organise the internal documents.

Purpose of Processing Organisation of training and conferences for external stakeholders, The carrying out of the Academy's statutory duties, To maintain a mailing list service and monitor users' preferences

Data Retention The retention period depends on the purpose for which the data is stored: category:
(a) "contact details for the mailing lists and alerts are kept until the data subjects unscribe themselves from the mailing list;
(b) events: until after the event and then the contact details of the self subscription are kept for mailing purposes (see category (a). Academy only keeps the contact details and delete the other data might have been collected;

(c) research programmes and schemes: the retained candidates data will be included in the Agreement and kept as long as the Agreement is kept according to the EPOs retention policy. (12 years. This is defined in the EPO's Codex, Part III, Chap 1B: FinRegs/Directive on Contracts, Art 9.5). Personal data of unsuccessful candidates are destroyed one year after submission but the email adresses will be kept for mailing purposes (category (a)).

(d) Audio visual material originating from events, is kept for a maximum period of 25 years.

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Country
Working email address	
Professional Experience & Affiliations	
CV	
Correspondence	
Additional Information which might be provided in the course of exchanges	Personal information provided voluntarily
Employment Information	
Business Unit Division	Language preference (of communication)
Personal Identification	
Full Name	
Education & Skills	
Education and Training History	Educational Degrees
Languages	

Employees

Contact Information	
Contact Details	Country
Working email address	
Correspondence	
Personal information provided voluntarily	
Employment Information	
Department name and/or number	Language preference (of communication)
Office Location	
Personal Identification	
Full Name	
Education & Skills	
Languages	

Recipient of the personal data

Recipients of the data Recipients from different operational units within the European Patent Office; for events (category (b) and research (category (c)) also recipients outside the EPOffice such as agencies or entities performing a peer review.

Purpose of sharing The purpose is to achieve the operational result for which the data is collected, such as the organisation and smooth running of the events and the performance of the research programme.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet
https://documents.epo.org/projects/babylon/eponet.nsf/0/83BF68AC46F67CEDC12588610031D23D/$File/data_protection_statement_on_the_processing_of_personal_data_within_framework_of_european_patent_academy_en.pdf

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 255

Name European Patent Administration Certificate (EPAC)

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 51 - Cooperation and Patent Academy

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

UNIwise

External processors	
Name UNIwise, UNIwise	

ServiceNow

External processors	
Name ServiceNow	

Description of the processing

Description Personal data is processed by the EPO to successfully organise and manage the European Patent Administration Certification and follow-up actions in accordance with the Rules concerning the establishment of a European Patent Administration Certification (EPAC) decided by the President of the EPO (pending).

The EPAC is a professional certification for patent administrators organised by the EPO. EPAC certifies the mastering of procedural administrative tasks relating to the patent granting procedures under the legal systems of the European Patent Convention (EPC) and the

Patent Cooperation Treaty (PCT).

The present document aims at providing information on how the personal data are processed in the context of the different stages and activities of EPAC, such as the enrolment of the candidates, the correct performance of the certification and the review process.

The European Patent Academy is in charge of the organisation and conduct of the EPAC. It shall decide on the result of each examination upon proposal of the EPAC Board, a certification support group in the sense of article 5 of Decision CA/D 7/21 of the Administrative Council of the European Patent Organisation.

These activities include the processing of personal data for candidates' enrolment and the payment of the fees.
Candidates with disabilities are flagged in the system as needing special arrangement, the medical details of the disability as such are not named nor stored, since only compensation is offered. Correspondence with candidate is kept in his/her file as long as the candidate is active in the EPAC.

EPAC can be done via an online platform or in presence.

The external supplier that provides the online platform process personal data on the EPO's behalf and it oversees the maintenance of the platform and offer support. The online platform has proctoring features to monitor the candidates during the examination to prevent attempts of fraudulent behaviour and keep proof of them, where deemed necessary.

Pursuant to Article 3(2) of the Rules concerning the establishment of EPAC, the EPAC Board is established for a three-year mandate and tasked with the drafting and marking of the EPAC examination. It shall make a proposal on the result of each examination to the Academy. The results are made available to each candidate.

According to Article 16 of the Rules concerning the establishment of EPAC, candidates' anonymity shall be respected when their answers are marked and their answers may be published for research, statistical or training purposes provided their anonymity is respected.

A review procedure before the EPAC review Board is possible in accordance with Articles 5 and 12 of the Rules concerning the establishment of EPAC. Candidates may request the review of a decision adversely affecting them. The request must be filed within a time limit of two weeks after notification of the decision and pay a review fee. The EPAC review board will inform the candidate of its decision in writing by electronic means. The decision of the EPAC review board is not subject to any further means of redress.

Members of the EPAC Board and EPAC review Board provide their data when becoming member

Purpose of Processing Administering EPAC which is a certification decided by the President within the framework of Decision CA/D 7/21 of the Administrative Council of the European Patent Organisation dated 13 October 2021 on modernising the structures of the European Patent Academy. Personal data are to be processed in order to: - decide whether the conditions to enrol are fulfilled - identify candidates - process payment - accurately associate candidates' answers, - keep previous results: if the first part has not been passed, the examination will be considered as failed and the other part(s) will not be marked. - ensure that EPAC is conducted properly (including technical support to the candidates by the EPO master users) and attempts of fraudulent behaviour are prevented or proven - process review requests - management of online candidate file - issue a certificate to successful candidates - publish a list of successful EPAC candidates as a searchable database on the website of the EPO. - select EPAC bodies members and manage their files

of the respective body.

Data Retention Depending on the categories of personal data processed, the personal data can be kept for different periods.

Personal data processed by the data controller or the service providers under its supervision are generally stored for the period necessary to achieve the purpose for which they have been processed. This applies to all documents and information obtained and produced in electronic and/or paper form in connection with a candidates' enrolment and participation in the EPAC.

Facial images, audio and biometric data produced from webcam and audio captures, the content of the communication (chat) will be retained by the processor's and sub-processors' systems for maximum 6 months.

In a case of suspected misconduct and/or review request the data, which are mentioned above as being retained by the processor and the sub-processors for a short period, will be copied and retained by the EPO in accordance with the Retention Policy

Data subjects and categories of personal data

Employees

Learning managements metrics	
Ratings	
Contact Information	
Contact Details	Country
Mobile Phone Number	Phone Numbers
Working email address	
Biometric	
Facial Recognition	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Examination content data	
Examination marks	Examination result
Online invigilation data	

Audio input	Webcam captures
Employment Information	
Language preference (of communication)	Office Location
Personal Identification	
Date of Birth	Disability or Specific Condition
Full Name	Gender
Nationality	Picture
Education & Skills	
Education and Training History	
Government Identifiers	
National Identity Card Details	Passport Number

Externals

Learning managements metrics	
Learning history	Ratings
Contact Information	
Contact Details	Country
Mobile Phone Number	Phone Numbers
Working email address	
Biometric	
Facial Recognition	
Correspondence	
Additional Information which might be provided in the course of exchanges	Chat content
Examination content data	
Examination marks	Examination result
Online invigilation data	
Audio input	Webcam captures
Employment Information	

Language preference (of communication)	
Personal Identification	
Date of Birth	Disability or Specific Condition
Full Name	Gender
Nationality	Picture
Education & Skills	
Education and Training History	Languages
Government Identifiers	
National Identity Card Details	Passport Number

Recipient of the personal data

Recipients of the data The EPAC Board and EPAC review Board have access to the data of candidates to the extent needed to perform their respective duties as defined in of the Rules concerning the establishment of EPAC.

Depending on the EPACQE body, access to the data is granted on a need-to-know basis to EPO and non-EPO staff.

According to Article 17 of the Rules concerning the establishment of EPAC, all EPO employees as well as external experts involved during and after their term of office shall be guaranteed with regard to all matters concerning EPAC and the candidates.
The personal data is disclosed, on a need-to-know basis, to the following recipients:
• the EPO's staff members of the European Patent Academy;
• members of the EPAC board and EPAC review Board;
• EPO authorised users (`master` users);
• Administrators of the WISEflow platform at UNIWise and its subprocessors (management of ticketing of incidents and to the following data of the candidates and the members of the Examination Committees for the bidirectional communication channel (chats) during the examination; hosting services);
• BIT
• Finance departments for the fee processing

Purpose of sharing Data is shared with the EPAC Board and the EPAC review Board. The purpose of sharing is the proper organisation and carrying out of the EPAC programme (examination and certification)

Transfer

Transfer Yes

Country where data might be transferred - Processor (Vendors) ServiceNow - Australia, ServiceNow - United States, ServiceNow - India, ServiceNow - Japan, ServiceNow - United Kingdom, UNIwise - United States

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards, Data Protection EU Comm Standard Contractual Clauses

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Treatment of data

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums)., To mitigate the risk of a conflict of interest within the EPO (EPO employees may sit the EPAC) access to data is restricted to a very limited group of persons. Technical means protect the violation of confidentiality as far as possible, even from system administrators. Technical staff of the service providers who cannot be exempted from access are individually known and bound by a confidentiality declaration. All personal data are stored in secure IT applications according to the security standards of the EPO. External providers are under strict contractual obligation as defined by Procurement and BIT standards. Limited access to data is given to technical staff of the provider on an event driven basis for the purpose of system administration and error analysis. For personal data processed on systems not hosted at EPO premises, a privacy

and security risk assessment has been carried out by the EPO. Except for a specific purpose defined in advance by the DPS, only the minimum necessary data are shared with other external parties. These parties have systems which are in conformity with the EPO security standards and have implemented the appropriate technical and organisational measures in this respect. All members of EPAC bodies are bound by secrecy under Article 17 of the Rules concerning the establishment of EPAC. Access to these data is protected by the personal user accounts of the members. Marking of the answers is anonymous. Financial procedures for the administration of fee payment are executed by the EPO Finance department and their service providers., For the data processing by UNIWise , UNIWise concluded a DPA , incl. EU SCCs, according to BIT

Data protection statement

Data Protection Statement link internet once approved by DPO

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 256

Name Organisation of Meetings between Legal Affairs and EPI

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities)

External processors

Zoom

External processors	
Name Zoom	

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft, Microsoft	

Description of the processing

Description Legal Affairs (PD52) holds regular meetings with representatives of the Institute of Professional Representatives before the EPO (epi) to discuss the cooperation between the EPO and epi.

Physical (or virtual) meetings are organised on an annual basis by PD52. When a meeting is being organised, an electronic file is created in the Case Management System (CMS) of the directorate under a specific log number together with the name of the responsible lawyer.

Legal affairs will provide details of the meeting to other participating directorates of the EPO. Legal Affairs will request the necessary information (agenda points, time schedule, etc.) from participants by email, and save that information in the corresponding CMS file.

The data is used by the EPO to organise the meeting and communicate related information to the participants or, on a need to know basis, to other stakeholders including:
*Technical aspects to be dealt with for the meeting itself (e.g. digital platform).
*Exchanges prior to the meeting e.g. preparation of the agenda, documents to be prepared and discussed.
*Exchanges after the meeting including sharing minutes, documents, possible follow-up actions.

The correspondence and documents exchanged before, during and after the meeting are saved in the CMS file. The Minutes of the meeting are then distributed to all participants of the meeting by email.

If applicable, notes or reports will be created after the meeting, including the name of the attendees, position and organisation represented, and distributed to the Hierarchy. In addition, documentation organising the meeting are stored on EPO Shared-Drive (W: drive) and CMS.

The active processing of personal data (mostly exchange of emails) stops after the end of possible follow-up actions/exchanges taking place after the meeting.

Data Retention Personal data necessary for organising meetings are kept until the next meeting has been organised.
The list of attendees and non-anonymised minutes are kept 10 years after the meeting.

Purpose of Processing Meetings between the Legal Division/EPO and epi are organised to discuss the collaboration between the Legal Division and epi. Personal data is processed to organise and facilitate the meetings, record the key conclusions of the meeting in the form of minutes, notes or reports (if applicable) and to distribute these conclusions to participants and the EPO hierarchy.

Data subjects and categories of personal data

Employees

General	
Any other information	
Contact Information	

Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Department name and/or number	Job Title Role
Personal Identification	
Full Name	Gender

Externals

General	
Any other information	
Contact Information	
Phone Numbers	Working email address
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Personal information provided voluntarily	
Employment Information	
Company Entity	Department name and/or number
Job Title Role	Language preference (of communication)
Office Location	
Personal Identification	
Digital signature	Full Name
Gender	

Recipient of the personal data

Recipients of the data Internal and external participants of the meeting.
Hierarchy of the EPO.
External processors.

Purpose of sharing Internal and external participants receive the minutes of the meeting, and any other personal data that is shared in the organisation of the meeting.
Hierarchy of the EPO receives minutes and if applicable notes or reports summarising the key conclusions from the meeting.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States, TRE Thomson Reuters - Luxembourg, Zoom - United States

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 269

Name Document design services

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 44 - General Administration

Entity Name - Processor (Entities) DG4 - 46 - CIO / BIT

External processors

Global Lingo

External processors	
Name Global Lingo	

Description of the processing

Description 1) Requests for document design work (such as the request concerning the transcriptions of oral proceedings or interviews or minutes, the formatting of documents, the creatiion of templates) are submitted by EPO staff or any department via the D 4.4.3.2 JIRA portal;
2) The Document Design Team (in 4.4.3.2) receives these requests under a ticket number as a link;
3) The requests are then processed internally or outsourced (transcriptions are always outsourced). In the case of outsourcing, data is sent via a generic Outlook mailbox (Document Design) to external contractors who return work via the same mailbox. An exception is outsourcing to the external provider GlobalLingo, provider for the GloZone service. GlobalLingo returns the completed transcriptions via the generic Outlook mailbox Document Design.
4) During the transcription/document design process, data (i.e. transcriptions as well as original and newly formatted files) are stored in JIRA under the ticket number. In the case of requests from 4.4.3 (concerning the formatting of documents), original and newly formatted files are also stored on Byblos.*
PPT presentations as well as many templates and files containing layout information are stored in an access-restricted folder on the W-Drive.

-> The process of storing transcriptions as well as formatted documents and the corresponding source files including any personal data contained therein is currently under review.

5) After completion of work, the transcriptions/formatted documents are sent back (as an attachment) to the requesters via the JIRA portal; requesters from 4.4.3 (editors/translators in 4.4.3.1) receive an email with a link to Byblos where the formatted documents and their original versions are stored.

Processing is partially automated.

* the requests/tickets are stored in JIRA and the link to the file on Byblos is/remains available in the request/ticket.

Data Retention The process of storing transcriptions as well as formatted documents and the corresponding source files including any personal data contained therein is currently under review.
In terms of storage periods, transcriptions will be kept for at least 1 year and all other requests/tickets for 5 years.

Purpose of Processing Process the request for document design work and for delivering the docuement

Data subjects and categories of personal data

Employees

Contact Information	
Contact Details	Home Address

Phone Numbers	Working email address
Professional Experience & Affiliations	
CV	
Employment Information	
Company Entity	Job Title Role
Personal Identification	
Full Name	Nationality
Signature	
Education & Skills	
Education and Training History	

Externals

Contact Information	
Contact Details	Home Address
Phone Numbers	
Professional Experience & Affiliations	
CV	
Employment Information	
Company Entity	Job Title Role
Previous Work History	
Personal Identification	
Full Name	Nationality
Signature	
Education & Skills	
Education and Training History	

Recipient of the personal data

Recipients of the data The personal data contained in the requested transcriptions and in documents sent for formatting is accessible only to the 4.4.3.2 staff members responsible for transcriptions and document design.

In the case of outsourcing, the personal data mentioned above is also accessible to external contractors.

In the case of formatting requests relating to documents which are edited and/or translated after/before formatting, the documents concerned are also accessible to the editors/translators in 4.4.3.1 as well as to external editors/translators in the case of outsourcing.

As for transcriptions/documents stored in JIRA, the tickets are accessible only to the 4.4.3.2 staff members responsible for transcriptions and document design and the application manager.

Purpose of sharing For outsourcing in the area of Document Design, a new contract is planned to be drawn up.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors) Global Lingo - United Kingdom

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 270

Name EPO Podcast

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 02 - Communication

Entity Name - Processor (Entities) DG4 - 41 - Finance, DG4 - 45 - CTO / BIT, DG4 - 47 - Procurement and Vendor Management

External processors

External audio-visual contractors

External processors	
Name External audio-visual contractors	

Description of the processing

Description

The EPO podcast aims to provide perspectives on innovation through interviews with experts, patent examiners, inventors or specialists in the commercialisation of innovation. The EPO collects and processes personal data from interviewers and interviewees to record and create the podcast.

For the organisation and creation of the script and recording of each podcast episode between the interviewer and the interviewees, the EPO manually collects, use and share personal data of the speakers of each podcast to the internal team in charge of the activity and the external provider which crate the audio material.

The recordings and other personal data, such as their names and personal pictures, are disclosed to the general public through different podcast platforms and the EPO internal and external channels. Podcasts are broadcasted through the EPO website on the following podcast platforms: Spotify, Stitcher, Google Podcasts, Apple Podcasts, Castbox, Deezer, PodBean, RadioPublic or TuneIn. Additionally, podcasts are used by the EPO for the promotion of each podcast episode through the EPO's internal and external channels, such as the intranet, the EPO website and all the EPO social media accounts. In addition, an episode of the EPO podcast might be shared and used by other multipliers when, for instance, the interviewee works for a company that also wants to promote this employee's interview through its channels.

The podcast audio files are normally not uploaded on the alternative platforms, they provide in the background the link to anchor.fm, our audio file repository. That said, some platforms may upload the podcast audio file too. The platforms cache the metadata (title, description, publication date, etc…) of the podcasts and store the personal data of their user and associate them with their favourite podcasts.

When users listen to the podcast on the EPO website or any third-party site, personal data may be collected and processed in accordance with the third parties' privacy policies. This applies especially if you listen to our podcast by having logged into one of the external podcast platforms mentioned here.

Personal data is also used for the payment of invoices.

Purpose of Processing Promotion, Payment to the speakers, Creation of the podcast

Data Retention Regarding the data used for the organisation and recording of each podcast episode, personal data not needed for the subsequent steps, such as mobile number or bank account (if applicable), will be deleted from the Principal Directorate Communication database once the invoice has been paid. Please bear in mind that some personal data are likely to remain in the EPO financial system for audit reasons.

Recordings and visual material used for the promotion of the EPO podcast are accessible to the public for a minimum period of three years. Nevertheless, Principal Directorate Communication may decide on a case-by-case basis to keep a podcast episode accessible for a longer period of up to seven years in order to provide the user with a satisfactory performance of the service.

If you use one of the platforms mentioned above, each platform keeps your data for as long as you are a user of their service.

In the event of a formal appeal/litigation, all data held at the time when the formal appeal/litigation was initiated will be kept until the proceedings have been concluded.

Data subjects and categories of personal data

Externals

Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Contact Details	Home Address
Personal Email	Phone Numbers
Working email address	
Financial	
Bank Account Information	
Travel & Expense	
Expense Details	
Browsing Information	
Cookie Information	IP Address
Network Interaction History	
Employment Information	

Company Entity	Job Title Role
Previous Work History	
Personal Identification	
Full Name	Gender
Surname	Nationality
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages

Employees

Sensory and Electronic Information	
Audio Information	Visual Information
Contact Information	
Contact Details	Personal Email
Phone Numbers	Working email address
Employment Information	
Company Entity	Contract Type
Job Title Role	Office Location
Personal Identification	
First Name	Full Name
Gender	Surname
Nationality	Signature
Education & Skills	
Education and Training History	Languages

Recipient of the personal data

Recipients of the data In addition to the EPO staff working in PDComm and the service provider entrusted by the EPO for the production of the audiomaterial, once published the personal data might be accessed by different stakeholders, such as
- podcasts's audience(EPO employees or external users of the podcast platforms and the EPO website)
- podcast platforms: Spotify, Stitcher, Google Podcasts, Apple Podcasts, Castbox, Deezer, PodBean, RadioPublic or TuneIn.
- Others, such as the speakers' employers.

Purpose of sharing Promotion of the EPO podcast

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, Service provider processing data for the creation of statistics

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet
https://www.epo.org/about-us/office/data-protection-and-privacy/epo-podcast.html

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 274

Name Invoicing

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 41 - Finance

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT

External processors

Jouve SAS

External processors	
Name Jouve SAS	

Description of the processing

Description The invoicing process comprises the processing of payment orders (invoices or reimbursements requests) issued by suppliers or beneficiaries. The process for both document types is identical thus both are called "invoices" in the following:
1. Invoices arrive via a common mail address as pdf. attachments to emails in the EPO mail rooms. The mail room staff is store the attachment on a FTP server.
2. Through this server, Jouve S.A., the EPO's outsourcing partner get access to the pdf invoices and converts them via optical character recognition form a pure image into an e-invoice readable for SAP (IDOC).
3. The IDOCs plus the image is fetched via the same FTP server and uploaded into VIM, a SAP solution for vendor invoice management.
4. In VIM, the actual invoice processing is taking place fully automated i.e. the automatic booking, formal compliance check, duplicate check and matching with the goods/service receipt by the responsible budget holder.
5. In case of exceptions, the automatic processing stops and VIM creates an error message specific to the exception.
6. If all steps under No.4 and No. 5 are completed the respective invoice is ready for payment when becoming due.
The invoicing process in the scope of this record comprises the steps No. 4 and 5

Data Retention 10 plus 1 year

Purpose of Processing Verification of invoices assuring correct and timely payments

Data subjects and categories of personal data

Externals

Contact Information	
Country	Home Address
Financial	
Bank Account Information	Bank Account Number
Bank details	Fund Reservation Requests
Travel & Expense	
Expense Details	
Employment Information	
Hours of Work	
Personal Identification	
First Name	Surname

Prospective Employees

Contact Information	
Country	Home Address
Financial	
Bank details	
Travel & Expense	
Expense Details	
Employment Information	
Job Application Details	
Personal Identification	
First Name	Surname

Contractors

Financial	
Fund Reservation Requests	
Travel & Expense	
Expense Details	
Employment Information	
Department name and/or number	Personnel Number
Personal Identification	
First Name	Surname

Employees

Financial	
Fund Reservation Requests	
Travel & Expense	
Expense Details	
Employment Information	
Department name and/or number	Personnel Number
Personal Identification	
First Name	Surname

Recipient of the personal data

Recipients of the data EPO Budget Holders/SIG 3, exceptionally Procurement Officers, very exceptionally with suppliers

Purpose of sharing Budget Holders/SIG 3 need to confirm the correctness of invoices thus it's often needed to share information disclosed on invoices with them.
Exceptionally, invoices are shared with Procurement Officers to clarify deemed differences in pricing and other contractual issues (EDP, VAT, payment terms etc.). The same applies for suppliers issuing the respective invoice.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors)

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet Will be implemented as soon as the data protection statement is completed

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 277

Name Data Protection Board - Case management for complaints lodged by external data subjects

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 52 - Legal Affairs

Entity Name - Processor (Entities) DG4 - 44 - General Administration

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft, Microsoft	

OpenText

External processors	
Name OpenText	

Description of the processing

Description As part of the means of redress available to data subjects, a complaint may be filed with the Data Protection Board against a decision by a delegated controller rejecting a

request for review (Article 50 of the Data Protection Rules). Upon receipt of a complaint, the Data Protection Board notifies the delegated controller author of the review decision. When complainants are not EPO staff members, the delegated controller liaises with PD52. PD52 provides in-house case-management and legal services and arrange the mandating of an external law firm to defend the position of the delegated controller in the proceedings.

This includes:
- arranging assistance and/or representation by an external law firm
- organising and maintaining the case file
- collecting relevant facts and evidence, analysing and advising on the case
- liaising with the delegated controller at stake
- preparing and/or checking submissions to be submitted to the Data Protection Board
- assisting in alternative dispute resolution attempts.

For this activity, personal data of the persons directly or indirectly involved in a complaint are processed, partly by automated means.

Information related to a case, including personal data, are collected via pleadings and evidence submitted from the parties to proceedings, third parties (e.g. witnesses), publicly available sources (e.g. internet searches), or
gathered from other Office's units in the course of fact-finding activities when preparing a case (e.g. delegated controller at stake, BIT...).

The personal data collected can be about the parties or others. The categories of personal data processed depends on the subject matter of a case and may occasionally include special categories of data.

Information related to a case is stored electronically in a document management system and in the electronic files kept by Legal Affairs. In some cases, a paper file is created.

Information related to a case are used in documents produced along the proceedings and exchanged between the parties or submitted to consultative (Data Protection Board) and decision-making (controller) bodies.

Information related to a case is shared within the Office as necessary for example to allow verification of factual elements, to inform or consult other services, to request translation, or in the course of approval or reporting process.

Information related to a case is transmitted outside the Office as necessary, for example when an external law firm is involved.

References to cases are included in lists kept for monitoring case statuses, for reporting and for statistical purposes.

Purpose of Processing Personal data is processed for the purpose of the EPO's administrative functioning, here in particular: 1- for assisting and/or advising and/or representing the delegated controller in the proceedings before the Data Protection Board 2- enabling the availability of complaint files for later reference in the event of subsequent litigation 3 – for archiving and statistical purposes.

Data Retention In the absence of a specific reason to retain a file:

Cases that proceeded to resolution by arbitration :
* 10 years after the arbitrator's final decision was pronounced, the parts of the file relating to the precedent stages of litigation are destroyed.
* 15 years after the arbitrator's final decision was pronounced, all parts are destroyed.

Other cases:
* 10 years after the closing of the complaint stage by withdrawal, unchallenged final decision or amicable settlement, all parts of the file other than the Data Protection Board's opinion and the final decision on the complaint are destroyed.
* 15 years after the closing of the complaint stage by withdrawal, unchallenged final decision or amicable settlement, all parts are destroyed.

This applies to both electronic and paper files.

An index of cases with limited personal data categories (reference, name, status) is kept indefinitely.

Data subjects and categories of personal data

Externals

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Representation in EPO’s Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)

Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Telephony Session Content	Telephony Session Details
Telephony Session Metadata	
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Nomination justificative	User association
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address

Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Ratings
Social learning inputs	
European Patent Register Data	
Address	Data provided by the data subjects
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	

System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Smart Card Number
Videoconference Room/Equipment Identifier	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Facial Recognition	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Employment Information	
Active/Inactive Indicator	Business Unit Division
Company Entity	Contract Type

Corporate Credit or Debit Card Numbers	Department name and/or number
Duration of employment	End Date
EPO access badge number	Hours of Work
Job Title Role	Language preference (of communication)
Membership in a EPO Staff Committee	Office Location
Previous Work History	Record of Maternity Leave
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Examination content data	
Examination marks	Examination result
Financial	
Bank Account Information	Bank Account Number
Bank details	Credit Card Number
Debit Card Number	Fund Reservation Requests
Information on home loans	Insurance Information
Browsing Information	

Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Membership Permissions
Ownership Permissions	Password Hash
Third-party User Identifier	User ID
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	

Employees

General	
Assessment and legal opinions	Legal opinions and assessments
Contact Information	
Contact Details	Working email address
Employment Information	
Assessment and legal opinions	
Personal Identification	
Full Name	Gender

Recipient of the personal data

Recipients of the data Personal data can be included in diverse communications or legal documents sent :
- to other operational units (such as delegated controller author of the review decision, Employment Law, Language Services...depending on the case, also to hierarchical line (VP5 assisted by CILO and President of the Office);
- to the Data Protection Board;
- possibly to external attorneys.

Purpose of sharing - to other operational units or staff members (such as delegated controller author of the review decision, Employment Law...): for fact-finding purposes, information and/or consultation on a strict need-to-know basis.
- Language Services: for obtaining a translation.
- Depending on the case at hand, personal data can be shared with the hierarchical line (VP5 assisted by CILO and President of the Office), for ex. for approval process and reporting purposes.
- to the Data Protection Board: for the conduct of the proceedings.
- possibly to external attorneys: for the conduct of the proceedings.

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation N.a.

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States, OpenText - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 281

Name Personal Data processing performed within the Logistic Centre activities - officewide -DG4 - PD 44 - General Administration

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 44 - General Administration

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft	

Courrier companies

External processors	
Name Courrier companies	

Description of the processing

Description The Logistics Centre is responsible for several activities within the EPO. The services requiring personal data collection, processing and storage are as follow:

1. Drivers / Transport
The requests are received by email, phone and the data subject must share email address, name, pick-up and drop-off location, timing for trip and mobile number. For a given trip, the driver details are also requested and stored.
In The Hague, the personal data are stored in SharePoint in the driver logbook.
In Munich, the personal data are deleted after the invoicing (between 1 to 4 weeks).

2. Printing Queue / Seal - Patent related
The formalities officer's and/or examiners request print work to be done using one of the patent tools which automatically get transferred to Plossys. From Plossys, the requests are sent to the printer by one staff of the logistic center. The request contains personal data of the requester (Staff ID and some personal data are contained in the document to be printed. In The Hague, external contractors proceed with the printing work. In Munich, the work is carried out by internal staff. A back-up of the printing works is kept in EPO ShareDrive. The data about printing are kept in order to prepare top management dashboard and/or in case of investigation.

3. Printing - other
Any staff within the EPO can request any work-related printing using Jira, email. The name, email address, phone number, office location are required.
Office-wide, once the work is delivered, the ticket is closed in JIRA and email is deleted in outlook.

4. Incoming Mail and parcels
Airbills is the tool registering all the incoming parcels and envelops that require signature from the recipient. The envelops or packages are scanned and the data transferred in Airbills containing the sender and recipient addresses, names, signatures.

5. Outgoing Mail and parcels
Regmail is the tool for outgoing registered parcels and envelops. The envelops or packages are scanned, and the data transferred in Regmail containing the recipient addresses, names. The courier service internet application is also used to ship parcels. The recipient address, email, phone number are entered to proceed with shipment.

6. Office supply
Office wide, stationaries are requested via EPO intranet stationary portal (http://apps.internal.epo.org/apps/officeSupplies/index.kerb.php).
The EPO staff select items for the order to be delivered and submit the request. The logistic center receives an automatic email containing: the name, the location, the phone number, and the content of the order. Once the delivery is done the request and related information are deleted.

Purpose of Processing The Logistics Centre needs to process personal data in connection with their daily activities and services delivery such as courier, printing, transport, office supplies… The data is registered to comply with some of the requirements established under several ISO standards on which the Office is either certified or in the process of being certified (e.g. PDCA improvement cycles of ISO 9001, 45001, 27001) as well as the follow up of risk logs that are part of those ones (e.g. ISO 45001).

Data Retention 1. Driver/Transport
The requests and associated personal data of the EPO staff are kept until the service is performed and invoice is received by the EPO, maximum 4 weeks.
For the driver, the data are kept for 1 year (in case of litigation, fines....).

2. Printing queue/seal - patent related
Plossys deletes automatically requests after execution (24hrs maximum), Back-up Data containing metadata (requester ID, addressee name and address) is stored 18 months

3. Printing - other
Requests are deleted after a maximum of 6 months.

4. Incoming Mail and parcels
Airbills data are kept 5 years and then automatically deleted (compliant with patent granting process)

5. Outgoing Mail and parcels
Regmail data are kept 5 years then automatically deleted (compliant with patent granting process)

6. Office supply
Outlook emails are kept until completion of the order for a maximum 6 months.

Data subjects and categories of personal data

Contractors

Contact Information	
Home Address	Mobile Phone Number
Phone Numbers	
Personal Identification	
Date of Birth	Full Name

Externals

Contact Information	
Phone Numbers	Working email address
Employment Information	
EPO access badge number	Office Location
Personal Identification	
Full Name	Signature
Unknown	

EPO badge validity	

Employees

Contact Information	
Home Address	Phone Numbers
Teleworking address	Working email address
Employment Information	
Office Location	Personnel Number
Room Number	
Personal Identification	
Full Name	Signature

Recipient of the personal data

Recipients of the data - Logistics Centre staff working on the activities described above.
- All contractors working on activities described above (transport companies, courier companies, drivers company's, post-offices, service contractors).

Purpose of sharing For execution of the requested activity.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 283

Name EPO E-Learning Centre

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG5 - 51 - Cooperation and Patent Academy

Entity Name - Processor (Entities) DG4 - 45 - CTO / BIT, DG4 - 46 - CIO / BIT

External processors

Xing

External processors	
Name Xing	

Description of the processing

Description The EPO E-learning Centre (also known as the Learning Management System (LMS)) is a platform that offers houses training courses to external users.
When a user registers with the e-learning centre, the user will be asked to provide certain personal data, which the EPO uses to identify the user. This includes a valid email address, which will be the user's user ID. The user will be able to modify the data (s)he enters, which will become the user's profile, at any time.

When registering for courses on the main EPO website (by using the online registration tool, which is a service provided by XING Events), the following personal data that the data subject (user) enters will be synchronised with the Learning Management System (LMS): first name, last name, city and country. The data subject's email address will be used as the user's unique identifier, i.e. will be the Data Subject's user ID.

The courses are free and no registration is required for the majority of courses. In that case, no personal data are collected.

If a user needs to register (and/or to pay) for a specific course, personal data is collected and the data subject is informed hereof, and the EPO does not proceed without the acceptance of the terms.

Data Retention Personal data is kept for as long as the user has an active account. The EPO will delete the account following a 1 year period of inactivity, or upon request of the user to cancel the account.

Purpose of Processing To create anonymised report on the platform's usage., To provide training, To collect information about the users' preferences and geographical distribution, To provide data subjects their progress

Data subjects and categories of personal data

Externals

Learning managements metrics	
Learning history	Learning plan
Contact Information	
Contact Details	Country
Personal Email	Working email address
Browsing Information	
Cookie Information	
Personal Identification	
First Name	Full Name
Surname	
Education & Skills	

Education and Training History

Recipient of the personal data

Recipients of the data Personal data might be shared with

- with the EPO staff and the contractors specifically selected;

- Tutors external to the EPO – hired on a contractual basis for a particular course

- the EPO's unit in charge of European and international co-operation and with the EPO's supervisory bodies.

- In the case of training specifically for staff of national patent offices in the European Patent Organisation's member states, with those national offices' EPO co-ordination officers as part of our co-operation with those offices.

Purpose of sharing The data is shared for the purposes of administering the platform and user support. For this, it will be shared with the EPO staff and the contractors specifically selected for these purposes.

- Tutors external to the EPO – hired on a contractual basis for a particular course – receive a list of that course's participants containing their first names, last names and countries.

- For EPO-internal planning and reporting, anonymised aggregated data may be shared with the unit in charge of European and international co-operation and with the EPO's supervisory bodies.

- In the case of training specifically for staff of national patent offices in the European Patent Organisation's member states, a list of participants in each training course is shared with those national offices' EPO co-ordination officers as part of our co-operation with those offices.

- Information on user preferences and users' geographical distribution collected to optimise technical improvements and for administering the platform and for support may be shared with EPO staff and contractors for these purposes.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network

Data protection statement

Data Protection Statement link internet once approved by DPO

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 286

Name Security documentation storage

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 44 - General Administration

Entity Name - Processor (Entities)

External processors

Microsoft

External processors	
Name Microsoft	

External HSE company

External processors	
Name External HSE company	

Description of the processing

Description The Security Sections of each EPO site register, archive, share and later on destroy any document required for the daily operation of the Security Services at the EPO. For this, they use the Security Document Management System (SDMS), which relies on a Microsoft SharePoint database and is split in three types of libraries with two types of documents each.
The types of libraries are the following:
1. Security Operations Documents: the library where the Security Sections at each EPO site archive their documents (both permanent and temporary documents). Those include incident reports, instructions, standard operating procedures, filled forms (e.g. COVID visitor registration forms), etc.
2. Technical Documents: the library where the Security Sections archive all service related requests, malfunctions on safety and security systems, fire alarm reports, stuck in elevator reports and any other ones that need to be shared with the OHS services for safety or Technical Service for maintenance and information.
3. Safety Documents: Any document, either permanent or temporary, related to health and safety issues. Those include, among others, the Office Emergency Response Plan, first aid reports, safety incident reports, emergency response team members lists, etc.
The types of documents per library are the following:
A. Permanent: documents which are needed on a permanent basis for the optimal operation of the services and have no retention policy applied (e.g. Circulars, instructions, guidelines, lists…etc.).
B. Temporary: documents drafted as a result of findings of the services which also have a retention policy applied per type of document, being automatically deleted afterwards (e.g. Incident reports, COVID visitor forms…etc.).
The accuracy of the personal data in these reports and documents is checked not only by EPO permanent staff but also by an external Quality Assurance Supervisor ("HSE company"), which ensures that only accurate data is processed and stored in this system.

Purpose of Processing Personal data is processed with the purpose of compliance with Circular 380, specifically Art. 2 b), whereby the President of the EPO has tasked Security Services to ensure compliance with the dispositions of that circular. The data registered serves to enhance the situational awareness of the security teams present in the office in view of providing security services and emergency assistance in an effective way to those present in case this would be needed. It is also used to register incidents and information (e.g. technical failures) that needs to be shared with other EPO departments.
Additionally, the data is registered to comply with some of the requirements established under several ISO standards on which the Office is either certified or in the process of being certified (e.g. PDCA improvement cycles of ISO 9001, 45001, 27001).

Data Retention The retention periods are mainly based in the duration of the security services contract, 5 years, and are established as follows:
1. SECURITY OPERATIONS
1.1. Temporary Documents are stored five years except the COVID visitors forms which are deleted after 14 days.
1.2. Permanent documents are stored until they get updated or are deemed not needed (e.g. Guideless on document design, instructions, list of first aiders or emergency response team members).
2. TECHNICAL DOCUMENTS
2.1. Temporary documents are stored for five years.
2.2. Permanent documents are stored until they get updated or are deemed not needed (e.g. Manuals, assessments and instructions)
3. SAFETY DOCUMENTS
3.1. Temporary documents are stored for five years.
3.2. Permanent documents are stored until they get updated or are deemed not needed (e.g. Manuals and instructions). If the list contains personal data (e.g. list of evacuation wardens or first aiders) then the file is reviewed and updated regularly but not deleted.

Data subjects and categories of personal data

Former Employees

Health Data	
Health Data	
Contact Information	
Mobile Phone Number	Personal Email
Unknown	
EPO badge validity	
Personal Identification	
Age	Date of Birth
Gender	

Contractors

Health Data	
Health Data	
Contact Information	
Working email address	
Building area and site	

Building area and site	
Employment Information	
Contract Type	Department name and/or number
End Date	EPO access badge number
Grade	Language preference (of communication)
Office Location	Room Number
Start Date	
Personal Identification	
Full Name	
Unknown	
EPO badge validity	Price list for discounts

Employees

Health Data	
Health Data	
Contact Information	
Working email address	
Building area and site	
Building area and site	
Employment Information	
Contract Type	Department name and/or number
Duration of employment	End Date
Grade	Job Title Role
Office Location	Start Date
Personal Identification	
First Name	Full Name
Gender	
Unknown	
EPO badge validity	Price list for discounts

Government Identifiers	
Car registration documents	

Externals

Health Data	
Health Data	
Sensory and Electronic Information	
Time stamps from their access to the buildings	
Contact Information	
Contact Details	Mobile Phone Number
Personal Email	
Unknown	
EPO badge validity	
Personal Identification	
Date of Birth	Full Name
Government Identifiers	
National Identity Card Details	

Recipient of the personal data

Recipients of the data 1. Security Operations documents are accessed by the Director and Heads of Department Facility Management as well as the EPO internal and external security services of PD44, with the exception of a part of the library named Quality Control that is only accessed by EPO internal staff (FM Director, HoD and Security Section permanent staff).
2. Technical Documents are accessed by the group number 1 above plus the EPO technicians in charge of the service of the installations and EPO Insurance Department staff, this last for analysis of risks and costs related to insurance.
3. Safety Documents are accessed by the same group as number 1 above plus Occupational Health and Safety Services staff.

Purpose of sharing The data is only used internally by FM security section staff and its external security contractor staff. If other recipients (e.g. Ethics and Compliance, Police, Safety Expert) request access to the personal data this will be individually asked to the Delegated Controller consulting DPO for advice.

Transfer

Transfer No

Country where data might be transferred - Processor (Vendors) Microsoft - United States

Transfer to public authority and/or International Organisation

Reasons for the transfer

Transfer mechanism(s)	Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures All personal data is processed and stored in IT applications (SharePoint) according to the security standards of EPO. These include: User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication; Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum; Logical security hardening of systems, equipment and network: 802.1x for network access, encryption of endpoint devices, AV on all devices Physical protection: EPO access controls, additional access controls to datacentre, policies to lock offices; Transmission and input controls (e.g. audit logging, systems and network monitoring): security monitoring with Splunk; Security incidence response: 24/7 monitoring for incidents, on-call security expert., For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 288

Name Job shadowing

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG4 - 421 - Talent Management

Entity Name - Processor (Entities) DG4 - 43 - Welfare & Remuneration

External processors

MyAbility

External processors	
Name MyAbility	

Description of the processing

Description The “MyAbility” job shadowing programme is organised by an external provider and takes place once a year with approximately 3 to 5 participants.

Young professionals/graduates can express their interest for a job shadowing at the EPO and in order to assess their profiles they give their explicit agreement to share some personal data with EPO representatives through an external provider where they would have applied beforehand.

Talents are asked in advance for their consent by the external service provider MyAbility to save their personal data (name, address, telephone number, email address, form of disability, status, field of study and companies to match with) which is a requirement for their participation.

The process comprises the following steps:
• During the application to the programme, registration at external provider (MyAbility): In order to participate in the programme, talents are asked in advance the consent to save their personal data in the external provider’s database (name, address, telephone number, email address, status, field of study and companies to match with) which is a requirement for their participation.
• Out of all the CVs collected, the external provider shares with EPO (PD4.3 and D4.2.1) all the applications received.
• Evaluation of profiles available excluding those that are not fitting the minimum requirement (depending on the job profile) and first assessment of possible fit with the business area is carried out by D421 and PD43
• Interview with pre-selected candidates who also expressed interest in the job shadowing with the organisation is carried out by D421 and PD43
• Outcome of the “matching day”. Specific number of profiles who passed the interviews and showed interest in the organisation. An Excel document with the pseudonymised profiles is created by D421 and PD43
• Recommendation of specific profile for specific area is made by D42.1 and PD43 to the EPO organisational units where the job shadowing is taking place.
• Once a candidate is nominated for a specific area, their information is shared with the line manager who is in charge /contact person for the job shadowing at the specific day.
• During the job shadowing event (information event for participants) (information is shared with all participants (email address is visible in the invitation to this event), communication department, security -in case of physical event.
• After the job shadowing event (email address, first and last name, physical address) a thank you email sent by internal organisers as well as a “goodie package” to the home address.

Purpose of Processing Young professionals/graduates can express their interest for a job shadowing at the EPO and in order to assess their profiles they give their explicit agreement to share some personal data with EPO representatives through an external provider where they would have applied beforehand. In order to be able to decide which of the talents shall participate to the Job shadowing day at the EPO, HR representatives as well as business representatives of the EPO need some relevant information available (academy qualifications, languages, CV, etc) to enable a proper evaluation of the profiles and to allow a first assessment of the matching with the business interest.

Data Retention Personal data will be kept only for the time needed to achieve the purposes for which it is processed.
Immediately after the event, Talent Acquisition (D4211) requests the involved stakeholders to delete the personal data.
Personal data will be deleted directly after the Job shadowing takes place.
I

Data subjects and categories of personal data

Externals

Contact Information	
Contact Details	Home Address
Personal Email	Private Phone Number
Correspondence	
Personal information provided voluntarily	
Personal Identification	
First Name	Surname
Education & Skills	
Education and Training History	

Recipient of the personal data

Recipients of the data Personal data are disclosed on a need-to-know basis to the EPO staff working in D 421 and PD 43 and the respective line manager of the organisational unit where the profile of the applicant could be considered suitable as well as to other units in order for these to carry out the necessary tasks to allow the job shadowing to take place.

Purpose of sharing Young professionals/graduates can express their interest for a job shadowing at the EPO and in order to assess their profiles they give their explicit agreement to share some personal data with EPO representatives through an external provider where they would have applied beforehand. In order to be able to decide which of the talents shall participate to the Job shadowing day at the EPO, HR representatives as well as business representatives of the EPO need some relevant information available (academy qualifications, languages, CV, etc) to enable a proper evaluation of the profiles and to allow a first assessment of the matching with the business interest.

Transfer

Transfer No

Transfer to public authority and/or International Organisation

Transfer mechanism(s)

Country where data might be transferred - Processor (Vendors)

Reasons for the transfer

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures All personal data are stored in secure IT applications in accordance with the EPO's security standards. Appropriate levels of access are granted individually only to the above-mentioned recipients. For systems hosted on EPO premises, the following basic security measures generally apply: • User authentication and access control (e.g. role-based access control to the systems and network, principles of need-to-know and least privilege) • Logical security hardening of systems, equipment and network • Physical protection: EPO access controls, additional access controls to datacentre, policies on locking offices • Transmission and input controls (e.g. audit logging, systems and network monitoring) • Security incident response: 24/7 monitoring for incidents, on-call security expert., For personal data processed on systems not hosted on EPO premises, the providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. These systems are required to have implemented appropriate technical and organisational measures such as: physical security measures, access and storage control measures, securing data at rest (e.g. by encryption); user, transmission and input control measures (e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging); conveyance control measures (e.g. securing data in transit by encryption)., In principle, the EPO has adopted a paperless policy management system; however, if paper files containing personal data need to be stored on EPO premises, they are locked in a secure location with a restricted access. When data are outsourced (e.g. stored, accessed and processed), a privacy and security risk assessment is carried out and the following general statement might be included in this field.	

Data protection statement

Data Protection Statement link internet	

Contact Details

Data controller: European Patent Office
Address: Bob-van-Benthem-Platz 1- 80469, Munich, Germany
Contact details: DPOexternalusers@epo.org
Data Protection Officer Name: Mariya Koleva
Data Protection Officer Contact Details: dpo@epo.org

Processing activity

ID 291

Name Processing of personal data within the framework of the Data Protection Board tasks, duties and activities

Delegated Controller and processor within the EPO

Entity Name - Controller (Entities) DG0 - 01 - Chief of Staff, President`s Office

Entity Name - Processor (Entities) DG0 - 07 - Data Protection Office

External processors

TRE Thomson Reuters

External processors	
Name TRE Thomson Reuters	

Microsoft

External processors	
Name Microsoft	

Data Protection Board Chair and Members

External processors	
Name Data Protection Board Chair and Members	

Description of the processing

Description The EPO’s Data Protection Board (DPB) processes personal data in order to carry out the tasks and duties assigned to it by the

Purpose of Processing Respond to consultations in the cases foreseen by the DPR. a. In the context of transfers of personal data to

Service Regulations for permanent and other employees of the EPO (Service Regulations), the DPR, Rules of Procedure of the Data Protection Board (RoP) and in compliance with additional operational documents governing the processing of personal data at the EPO.

The DPB fulfils a monitoring and an advisory function by providing opinions and advice on data protection related matters in response to requests for consultation from the controller, the delegated controller(s) and the EPO Data Protection Office (DPO) in the cases foreseen by the DPR. For more information on the processing of personal data by these parties, please refer to the relevant records.

Furthermore, the DPB provides an opinion where data subject files a complaint before the DPB as part of the legal redress procedure under Article 50 DPR (hereinafter “complaint proceedings”). For more information on the complaint proceedings procedure, please refer to the Rules of Procedure (RoP).

In the performance of its tasks, the DPB may process any category of personal data (including special categories of personal data) provided by EPO staff members or externals regarding themselves or third parties
in the context of the complaint proceedings. It includes information exchanged such as the description of concerns, personal case, circumstances, description of facts, evidence or arguments, opinions, assessments, etc.

Personal data are processed by the secretariat of the DPB, which is made available by the EPO (DPO), in order to assist the Chair, members and alternate members in carrying out the tasks and duties of the DPB referred to in this statement. Furthermore, the DPO might process personal data when acting upon request of the DPB in accordance with the tasks and responsibilities established under the DPR.

Personal data may be stored in one or more document management tools used by the DPB to perform its tasks, namely on the EPO’s servers and/or in Microsoft Office cloud systems:

- all consultations, requests, opinions, other exchanges and related communications (together with supplementary documentation, as the case may be) received or sent by the DPB are stored in Outlook in folders separated by year and/or on SharePoint 2019 and are only accessible to authorised staff;
- opinions in the context of complaint proceedings and related documentation are additionally archived in the EPO document management tool (MatterSphere) with a specific number assigned to them;
- opinions of the DPB outside of complaint proceedings, redacted abstracts from the final decisions of the controller and the opinions of the DPB in the context of complaint proceedings may also be published on the EPO intranet and/or externally, and be made available to all staff and the general public.

third countries and international organisations: - The DPB may provide an opinion to the President of the Office on whether the protection afforded by said third country or international organisation can be considered as adequate (Article 9(3) DPR). - In the absence of an adequate level of protection, the DPB may be consulted by the controller on the drafting of appropriate contractual clauses aiming to provide appropriate safeguards for the transfer (Article 9(5) DPR). b. In the context of Data Protection Impact Assessment (DPIA) as established by Article 38 DPR: - The DPO or the controller will consult the DPB if there is a doubt on the need to perform a DPIA (Article 43(1)(g) and 38(2) DPR). - The DPB will draw a list of the kinds of processing operations for which a DPIA is required (Article 47(2)(b) DPR). c. In the context of the removal of the Data Protection Officer from their role or termination of their appointment, the DPB provides an opinion on such removal or termination (Article 42(8) DPR). d. In the context of processing of data relating to criminal offences, criminal convictions or security measures based on Article 5(a) DPR, the DPB may need to be consulted before such processing may be carried out (Article 12(1) DPR)., Provide an opinion where data subject files a complaint before the DPB as part of the complaint proceedings. In the context of complaint proceedings personal data are processed for the following purposes: a. to register the complaint filed before the DPB using the appropriate form and to determine its receivability as foreseen by Article 5 RoP b. to forward the complaint and the attached documents (if any) to the delegated controller responsible for the processing operation which relates to the complaint, authorised parties involved in the defence of the EPO, the DPO and, where applicable, the processor in order for them to be informed of the complaint and to prepare their submissions as applicable c. if the case may be, to facilitate an amicable settlement as described in Article 8 RoP d. to provide the DPB with adequate and sufficient information to enable it to render an opinion e. if required by the circumstances of the complaint, upon the authorisation of the President of the EPO and in accordance with the Protocol on Privileges and Immunities as applicable, to co-operate with the competent national authorities, including competent national supervisory authorities or law enforcement authorities f. upon the authorisation of the President of the EPO and in accordance with the Protocol on Privileges and Immunities as applicable, to share with a court or another judicial or administrative body in the event of a suspension of complaint proceedings before the DPB pending a ruling on the same matter from the said body g. to share the reasoned opinion of the DPB with the controller and the parties involved in the procedure, including the complainant(s), legal representative(s) (if any), delegated controller(s) and authorised parties involved in the defence of the EPO and the DPO h. to archive the opinion and the final decision of the controller, rendered after reception of DPB’s reasoned opinion on SharePoint 2019 and MatterSphere redacted abstracts from the final decision and from the opinion of the DPB may be published internally

For more information regarding the processing of personal data by these tools, please refer to the dedicated record(s).

The processing is not intended to be used for any automated individual decision-making.
Data Retention Personal data will be kept only for the time needed to achieve the purposes for which they are processed.

Personal data related to consultations and other exchanges will be stored in the document management tool(s) for a maximum of 5 years after the end of the consultation or end of the exchange. Opinions that are published online will be stored as long as they are operational. Upon becoming obsolete, the documents will be taken down, anonymised and archived in the document management tool(s) for an additional period of 5 years.

Personal data related to the complaint proceedings under Article 50 DPR will be stored in the document management tool(s) for a maximum of 10 years after the complaint had been withdrawn, found irreceivable or definitively resolved through a final decision taken by the controller which has not been challenged; a judgment by the Administrative Tribunal of the International Labour Organisation; a judgment issued in dispute resolution proceedings under Article 50(7) of the DPR; an arbitration award rendered in ad-hoc arbitration proceedings under Article 50(8) and 52 DPR; or an amicable settlement.

Members of the DPB shall destroy and/or erase any files or copies of files pertaining to a complaint case file within 6 months of the issue of the DPB’s opinion.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

and/or externally by the secretariat of the DPB, Cooperate with EPO units, facilitated by the DPO, in particular with regard to organisational or other developments that are likely to have an impact on the protection of personal data within the EPO, including new administrative measures and rules.

Data subjects and categories of personal data

Contractors

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information

Presence Status	Thermal Information
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Representation in EPO’s Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History

Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Assessment and legal opinions	Input provided during the deliberation and decision-making process
Legal opinions and assessments	Nomination justificative
User association	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Previous Residence Address
Private Phone Number	Teleworking address
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID

Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	

Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Pod Internal Id
Smart Card Number	Videoconference Room/Equipment Identifier
Workstation Serial Number	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Active/Inactive Indicator	Appeals Records Information
Assessment and legal opinions	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	Disciplinary Action
Duration of employment	End Date
End Date and Reason for Termination	EPO access badge number
Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Title Role

Language preference (of communication)	Line Reporting Manager
Membership in a EPO Staff Committee	Military Status
Office Location	Performance Rating
Personnel Number	Previous Work History
Record of Absence/Time Tracking/Annual Leave	Record of Maternity Leave
Room Number	Salary
Start Date	Weight
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Results on phishing attempts (entered credential not processed)	Session content
Session details	Session metadata
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Examination content data	
Examination marks	Examination result
Financial	
Bank Account Information	Bank Account Number

Bank details	Bank Statements
Bonus Payments	Compensation Data
Credit Card Number	Credit History
Debit Card Number	Deposit Account
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Application Specific User Role
Membership Permissions	Ownership Permissions
Password	Password Hash
Third-party User Identifier	User ID
Government Identifiers	
Driving Licence Number	ID/Passport picture
National Identification Number	National Identity Card Details
Passport Number	Social Security Number

Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact

Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Thermal Information
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Representation in EPO’s Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs

Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Assessment and legal opinions	Input provided during the deliberation and decision-making process
Legal opinions and assessments	Nomination justificative
Personal data in SAP	Sensitive Personal Data in SAP
Special categories of personal data in SAP	User association
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Home Leave Address	Mobile Phone Number
Personal Email	Phone Numbers
Previous Residence Address	Private Phone Number
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
Diagnostic tools’ results	IDP
Instructor related data	Learning external events
Learning history	Learning plan

Ratings	Social learning inputs
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number

Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Pod Internal Id
Smart Card Number	Videoconference Room/Equipment Identifier
Workstation Serial Number	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Active/Inactive Indicator	Appeals Records Information
Assessment and legal opinions	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Corporate Credit or Debit Card Numbers
Department name and/or number	Disciplinary Action
Duration of employment	End Date

End Date and Reason for Termination	EPO access badge number
Exit Interview and Comments	Grade
Grievances and Complaints	Hours of Work
Job Application Details	Job Group
Job Title Role	Language preference (of communication)
Line Reporting Manager	Membership in a EPO Staff Committee
Military Status	Office Location
Performance Rating	Personnel Number
Previous Work History	Record of Absence/Time Tracking/Annual Leave
Record of Maternity Leave	Rewards history
Room Number	Salary
Start Date	Weight
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Results on phishing attempts (entered credential not processed)	Session content
Session details	Session metadata
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV

Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Examination content data	
Examination marks	Examination result
Family Information	
Child’s Level/Year of Studies	Child’s School Enrolment Date Start
Children's Names	Child's birthday
Composition of the family (number of dependent children/persons)	Parents' Names
Spouse's information	Spouse's name
Financial	
Bank Account Information	Bank Account Number
Bank details	Bank Statements
Bonus Payments	Compensation Data
Credit Card Number	Credit History
Debit Card Number	Deposit Account
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number

Account Password	Application Specific User Role
Membership Permissions	Ownership Permissions
Password	Password Hash
Third-party User Identifier	User ID
Government Identifiers	
Car registration documents	Driving Licence Number
ID/Passport picture	National Identification Number
National Identity Card Details	Passport Number
Social Security Number	

Externals

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Time stamps from their access to the buildings
Visual Information	
Building area and site	
Building area and site	
Representation in EPO’s Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	

Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Surname
Nationality	Picture
Signature	
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Nomination justificative	User association
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number

Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Ratings
Social learning inputs	
European Patent Register Data	
Address	Data provided by the data subjects
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)

Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name
Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Smart Card Number
Videoconference Room/Equipment Identifier	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Biometric	
Facial Recognition	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Employment Information	
Active/Inactive Indicator	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Duration of employment	End Date

EPO access badge number	Hours of Work
Job Title Role	Language preference (of communication)
Membership in a EPO Staff Committee	Office Location
Previous Work History	Record of Maternity Leave
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Examination content data	
Examination marks	Examination result
Financial	
Bank Account Information	Bank Account Number
Bank details	Credit Card Number
Debit Card Number	Deposit Account
Fund Reservation Requests	Information on home loans
Insurance Information	

Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Application Specific User Role
Membership Permissions	Ownership Permissions
Password Hash	Third-party User Identifier
User ID	
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	

Former Employees

Applications' Log	
SAP Logs	
Social	
Social Media Account	Social Media Contact
Social Media History	
Sensory and Electronic Information	
Audio Information	Electronic Information
Presence Status	Thermal Information
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Representation in EPO’s Patent Granting Process	

Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Racial or Ethnic Origin	Religion/Religious Beliefs
Sexual Orientation	Signature
Education & Skills	
Academic Transcripts	Education and Training History
Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	

Answers to surveys, assessments or quizzes	Any other information
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Nomination justificative	Personal Information in SAP
Sensitive Personal Data in SAP	Special Categories of Data in SAP
User association	
Workplace Welfare	
Records of Personal Properties	
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Home Leave Address	Mobile Phone Number
Personal Email	Phone Numbers
Previous Residence Address	Private Phone Number
Teleworking address	Working email address
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs

Tenant ID	Windows ID for Windows Devices
Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
Patent Process Related Data	
Patent Record Bibliographic and Meta Data	Personal data potentially included within the content of a patent (claims, description, drawings, abstract)
Personal data potentially included within the content of patent procedure related information and publications	
Health Insurance Information	
Insurance Policy Information	Unique Identifier for Subscriber
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
Digital Certificate	ICCID (Integrated Circuit Card Identification Number)
IMEI Number (International Mobile Equipment Identity)	Mobile Device Name

Mobile Device Serial Number	Mobile Device's Network Adapter MAC Adress
Operating System Version	Pod Internal Id
Smart Card Number	Videoconference Room/Equipment Identifier
Workstation Serial Number	Workstation's Hostname (Physical or Virtual)
Workstation's Network Adapter MAC address	
Biometric	
Body temperature	Facial Recognition
Fingerprint	Voice Recognition
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks
Employment Information	
Active/Inactive Indicator	Appeals Records Information
Benefits and Entitlements Data	Business Unit Division
Company Entity	Contract Type
Corporate Credit or Debit Card Numbers	Department name and/or number
Disciplinary Action	Duration of employment
End Date	End Date and Reason for Termination
EPO access badge number	Exit Interview and Comments
Grade	Grievances and Complaints
Hours of Work	Job Application Details
Job Group	Job Title Role
Language preference (of communication)	Line Reporting Manager
Membership in a EPO Staff Committee	Military Status
Office Location	Performance Rating

Personnel Number	Previous Work History
Record of Absence/Time Tracking/Annual Leave	Record of Maternity Leave
Rewards history	Room Number
Salary	Start Date
Weight	
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Geolocation	
Geolocation Information	
Network/application Interaction Data	
Results on phishing attempts (entered credential not processed)	Session content
Session details	Session metadata
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications
Trade Union Membership	
Examination content data	
Examination marks	Examination result
Family Information	
Children's Names	Parents' Names
Spouse's information	Spouse's name
Financial	

Bank Account Information	Bank Account Number
Bank details	Bank Statements
Bonus Payments	Compensation Data
Credit Card Number	Credit History
Debit Card Number	Deposit Account
Fund Reservation Requests	Information on home loans
Insurance Information	Routing Number
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Application Specific User Role
Membership Permissions	Ownership Permissions
Password	Password Hash
Third-party User Identifier	User ID
Government Identifiers	
Driving Licence Number	ID/Passport picture
National Identification Number	National Identity Card Details
Passport Number	Social Security Number

Prospective Employees

Applications' Log	
SAP Logs	
Social	

Social Media Account	Social Media Contact
Sensory and Electronic Information	
Audio Information	Presence Status
Time stamps from their access to the buildings	Visual Information
Building area and site	
Building area and site	
Representation in EPO’s Patent Granting Process	
Affiliation to Association of professional representatives	All data provided upon request for entry or change
Authorisee function	Authorisor function
EPO CDS (Client Data System) categories related to the Representation role	Representative registration number (ID)
Role in the Patent Grant Procedure	Supporting documentation
Telephony Interaction Data	
Recorded Audio File	Telephony Session Content
Telephony Session Details	Telephony Session Metadata
Travel & Expense	
Expense Details	Travel Booking Details
Travel History	
Personal Identification	
Age	Date of Birth
Digital signature	Disability or Specific Condition
First Name	Full Name
Gender	Height
Surname	Marital Status
Nationality	Picture
Religion/Religious Beliefs	Signature
Education & Skills	
Academic Transcripts	Education and Training History

Educational Degrees	Languages
Project management experience	
Matter/Log file	
Attachments	Metadata
General	
Answers to surveys, assessments or quizzes	Any other information
Input provided during the deliberation and decision-making process	Legal opinions and assessments
Nomination justificative	User association
Contact Information	
Contact Details	Country
Emergency Contact Details	Home Address
Mobile Phone Number	Personal Email
Phone Numbers	Private Phone Number
Working email address	
Learning managements metrics	
Answers to surveys/Assessments/Quizzes	Coach related data
IDP	Instructor related data
Learning external events	Learning history
Learning plan	Social learning inputs
Device Management Data	
Account ID	AppleID for iOS/iPadOS Devices
Azure Active Directory Device ID	EAS Device ID
Encryption Keys	Intune Device ID
Intune Device Management ID	Last Logon Time
MAC Address	Managed Application Device Tag
Managed Application ID	Platform-specific IDs
Tenant ID	Windows ID for Windows Devices

Correspondence	
Additional Information which might be provided in the course of exchanges	Any other information
Chat content	Personal information provided voluntarily
System Logs	
Audit Logs (a.k.a. Audit Trail)	File data (name, size and/or hash)
Firewall/Router/Switch Logs	Ports
Registry data	Running Processes
System-, Application-, Security-related Server Logs	Transaction-related Details
Web Servers Logs	
Phone Call Information	
Called Phone Number	Caller's Phone Number
Phone Call Date and/or Time	Phone Call Duration
Phone Call Interaction History	Phone Calling History
Ticketing	
Ticket related data	
Physical and/or Digital Identifiable Assets	
ICCID (Integrated Circuit Card Identification Number)	IMEI Number (International Mobile Equipment Identity)
Mobile Device Name	Mobile Device Serial Number
Mobile Device's Network Adapter MAC Adress	Operating System Version
Videoconference Room/Equipment Identifier	Workstation Serial Number
Workstation's Hostname (Physical or Virtual)	Workstation's Network Adapter MAC address
Online invigilation data	
Audio input	Webcam captures
Background Checks	
Criminal History	Criminal Records
Drug Test Results	Reference or Background Checks

Employment Information	
Active/Inactive Indicator	Benefits and Entitlements Data
Business Unit Division	Company Entity
Contract Type	Department name and/or number
Duration of employment	End Date
End Date and Reason for Termination	EPO access badge number
Grade	Job Application Details
Job Group	Job Title Role
Language preference (of communication)	Line Reporting Manager
Membership in a EPO Staff Committee	Military Status
Office Location	Performance Rating
Previous Work History	Record of Maternity Leave
Rewards history	Salary
Start Date	Weight
Unknown	
EPO badge validity	Identification of which membership is envisaged
Price list for discounts	
Network/application Interaction Data	
Session content	Session details
Session metadata	
Health Data	
Dietary requirements	Health Data
Mobility needs	
Professional Experience & Affiliations	
Affiliation	CV
Entry or deletion date as member of an association	Political Affiliation and Activities
Professional Memberships	Qualifications Certifications

Examination content data	
Examination marks	Examination result
Financial	
Bank details	Deposit Account
Fund Reservation Requests	Information on home loans
Browsing Information	
Browser type	Browser User Agent
Browsing Date and Time	Browsing Time
Category	Cookie Information
IP Address	Network Interaction History
URL	Website History
User Account Information	
Account Age	Account Number
Account Password	Application Specific User Role
Membership Permissions	Ownership Permissions
Password	Password Hash
Third-party User Identifier	
Government Identifiers	
ID/Passport picture	National Identity Card Details
Passport Number	

Recipient of the personal data

Recipients of the data Personal data may be disclosed to the Chair, members, alternate members and the secretariat of the DPB on a need-to-know basis and only to the extent necessary to carry out tasks and duties of the DPB. Additionally, personal data are disclosed to below mentioned recipients.

In the case of consultations, personal data may be disclosed to the controller, the delegated controller(s) responsible for the processing operation related to the consultation (including their respective Data Protection Liaisons (DPLs) if necessary), and the DPO. Strictly necessary personal data may be shared with other authorised EPO staff on a strict need-to-know basis to collect and compile information necessary for the DPB to form an opinion regarding the consultation.

In the case of exchanges with the DPO and the EPO units in particular with regard to developments likely to have impact on the processing of personal data at the EPO, personal data may be disclosed to the DPO and other authorised EPO staff involved in the exchange.

In the case of complaint proceedings personal data may be disclosed, on the need-to-know basis:
- to the parties involved in the procedure, including the complainant(s), legal representative(s) (if any), delegated controller(s), the controller, authorised parties involved in the defence of the EPO, and, where applicable, the processors, as well as to the DPO
- to the DPO and other parties that may be invited as observers during meetings of the DPB regarding the complaint
- to competent national authorities, including competent national supervisory authorities or law enforcement authorities acting within the scope of their respective competences when required by the circumstances of the complaint
- to a court or another judicial or administrative body in the event of a suspension of complaint proceedings before the DPB pending a ruling on the same matter from the said body
- to other authorised EPO staff only to the extent necessary to handle the complaint

Personal data may be stored in one or more document management tools used by the DPB to perform its tasks, notably: MatterSphere, Microsoft Outlook and SharePoint 2019. Personal data will be stored and made available in these applications strictly on a need-to-know basis and for no longer than needed to achieve the purposes for which they are processed. For more information regarding the processing of personal data by these tools, please refer to the specific data protection statements.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

Purpose of sharing - To respond to consultations in the cases foreseen by the DPR
- To cooperate with EPO units, facilitated by the DPO, in particular with regard to organisational or other developments that are likely to have an impact on the protection of personal data within the EPO, including new administrative measures and rules
- To provide an opinion where data subject files a complaint as part of the legal redress procedure under Article 50 DPR

Transfer

Transfer Yes

Transfer to public authority and/or International Organisation In the case of complaint proceedings personal data may be transferred outside the EPC contracting states:
- to competent national authorities, including competent national supervisory authorities or law enforcement authorities acting within the scope of their respective competences when required by the circumstances of the complaint
- to a court or another judicial or administrative body in the event of a suspension of complaint proceedings before the DPB pending a ruling on the same matter from the said body

Transfer mechanism(s) The recipient provided appropriate safeguards

Country where data might be transferred - Processor (Vendors) Microsoft - United States, TRE Thomson Reuters - Luxembourg

Reasons for the transfer Service provider processing data only for Operations/Maintenance purposes, In the context of the complaint proceedings when required by the circumstances of the complaint

Derogations Art. 10 DPR

Organisational and security measures

Organisational and security measures EPO personal data are processed in secure IT applications according to the security standards of EPO. These include: * User authentication: all workstations and servers require login, mobile devices require login to the EPO enclave, privileged accounts require additional and stronger authentication. * Access control (e.g. Role-based access control to the systems and network, principles of need-to-know and least privilege): separation into administrative and user roles, users have minimum privileges, reduction of overall administrative roles to a minimum. * Logical security hardening of systems, equipment and network: 802.1x for network, For personal data processed on systems not hosted at EPO premises, a privacy and security risk assessment has been carried out by the EPO. These systems are required to have implemented appropriate technical and organisational measures such as: * Physical security measures. * Access control measures: role-based, principles of need-to-know and least privilege. * Storage control measures: access control e.g. role-based, principles of need-to-know and least privilege, Securing data at rest e.g. by encryption, Secure disposal of data carriers. * User control measures: network security measures e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), Host security measures e.g. antivirus, anti-malware, anti-spyware, whitelisting, host firewall, host IDS, host IPS, System hardening, Vulnerability and patch management; * transmission control measures: audit logging, System and network monitoring; * Input control measures: audit logging, System monitoring; * Conveyance control measures: securing data in transit e.g. by encryption, Data validation e.g. by using of HMAC (keyed-hash message authentication code), hashes and checksums).

Data protection statement

Data Protection Statement link internet
http://my.internal.epo.org/portal/private/epo/organisation/dg0/?WCM_GLOBAL_CONTEXT=/epo/intranet/organisation/dg0/d_dpo/legal_redress/1655908534590_dpb_data_protection_statements