Déclaration relative à la protection des données concernant le traitement de données à caractère personnel dans le cadre de Splunk

Pour l'Office européen des brevets ("OEB"), la protection de votre vie privée est de la plus haute importance. Nous nous engageons à protéger vos données à caractère personnel et à veiller au respect des droits des personnes concernées lorsque nous accomplissons nos tâches et fournissons nos services. Toutes les données à caractère personnel qui permettent de vous identifier directement ou indirectement seront traitées conformément à la loi, de façon équitable et avec une diligence raisonnable.

Les opérations de traitement décrites ci-après sont régies par le règlement relatif à la protection des données (RRPD) de l'OEB.
Les informations contenues dans la présente déclaration sont fournies en vertu des articles 16 et 17 RRPD.

Splunk est le référentiel central des fichiers journaux de l'OEB pour la gestion des incidents de sécurité. Il assure la protection des systèmes de l'OEB en facilitant l'identification et l'analyse des problèmes de sécurité.

1. Quelles sont la nature et la finalité des opérations de traitement ?

Le traitement des données à l'aide de Splunk comprend les éléments suivants :

- réception des données techniques générées et déjà disponibles auprès d'autres systèmes et services de BIT
- réalisation de requêtes automatisées afin de générer des alertes associées à des événements de sécurité
- réalisation de requêtes automatisées afin de générer des tableaux de bord et des vues d'ensemble associés aux informations de sécurité
- réalisation de requêtes manuelles pour l'analyse approfondie des événements de sécurité, l'adaptation des tableaux de bord et l'émission d'alertes

Splunk reçoit des données techniques générées par (et disponibles sur) un certain nombre de systèmes et services de l'OEB, notamment :

- des postes de travail gérés par l'OEB assignés à des utilisateurs de l'OEB ;
- des serveurs gérés par l'OEB ;
- des équipements de réseau gérés par l'OEB (p. ex. : routeurs, commutateurs, pare-feu et serveurs proxy) ;
- des prestataires externes de services cloud disposant d'une relation contractuelle établie avec l'OEB (p. ex. : Microsoft, Google, Amazon et SAP).

Les données à caractère personnel sont traitées dans le but d'identifier les personnes ayant réalisé les activités qui ont été enregistrées, afin d'analyser les éventuels incidents de sécurité ou erreurs détectés. C'est important car :

- les fichiers journaux sont utilisés pour réaliser le suivi des événements dans un système d'information et faciliter le débogage et les réparations. Ils font partie du système et sont indispensables pour assurer la sécurité et un support efficace lorsque les systèmes d'information ne fonctionnent pas correctement ;
- les fichiers journaux des systèmes de l'OEB sont traités pour analyser et résoudre les incidents de sécurité et les infections par logiciels malveillants concernant des appareils connectés au réseau de l'OEB, et/ou pour prévenir les fuites de données ;
- de plus, les fichiers journaux peuvent être traités dans un but statistique ou pour résoudre les problèmes d'accès des utilisateurs aux systèmes de télécommunication de l'OEB.

Le traitement ne doit faire l'objet d'aucune prise de décision automatisée, y compris un profilage.

Les données personnelles vous concernant ne seront pas communiquées à d'autres destinataires en dehors de l'OEB.

2. Quelles sont les données à caractère personnel traitées par l'OEB ?

Via Splunk, le responsable délégué du traitement, la DP BIT 4.6, collecte des données à caractère personnel, dès que et quand ces données sont incluses dans les journaux générés par le système d'origine. Aucune catégorie spéciale de données à caractère personnel n'est collectée sciemment ou volontairement via Splunk.

Les données à caractère personnel traitées peuvent se rapporter au personnel de l'OEB, à des sous-traitants de l'OEB ou à des utilisateurs extérieurs.

Données à caractère personnel traitées si la personne concernée fait partie du personnel de l'OEB ou est un sous-traitant :

- données d'identification personnelle : nom complet (prénom + nom de famille) et genre
- coordonnées : adresse électronique professionnelle, numéros de téléphone
- informations du compte utilisateur : identifiant, numéro de compte
- données d'interaction avec le réseau/l'application : métadonnées de session
- journaux système : processus en cours d'exécution, données de registre, métadonnées de fichier (nom, taille, hachage du fichier), numéros de port, détails de transaction, journaux d'audit, journaux de serveurs associés au système, à l'application et à la sécurité, journaux de serveurs web, journaux de pare-feu, de routeurs, de commutateurs
- identifiants d'équipements physiques/numériques que la personne concernée a utilisés pour se connecter aux systèmes de l'OEB : numéro de série, nom d'hôte et adaptateur réseau du poste de travail, adresse MAC, version du système d'exploitation
- informations de navigation : type de navigateur, URL, agent utilisateur du navigateur, date et heure de navigation, adresse IP, catégorie, historique du site web, historique des interactions réseau
- informations relatives aux appels téléphoniques : numéro de l'appelant, numéro appelé, date et heure, durée, historique des interactions
- données d'interaction téléphoniques : métadonnées de session téléphonique
- informations relatives à l'emploi : indicateur actif/inactif, données de fin, nom et/ou numéro de département, numéro de bureau, emplacement du bureau, titre, groupe d'emplois (personnel uniquement), date de début, supérieur hiérarchique, préférence de langue (pour la communication), type de contrat, numéro personnel
- données associées au ticket
- informations de géolocalisation

Données à caractère personnel traitées si la personne concernée est externe :

- données d'interaction avec le réseau/l'application : métadonnées de session
- journaux système : journaux de pare-feu/routeurs/commutateurs, journaux de serveurs web, journaux de serveurs associés au système, à l'application et à la sécurité
- identifiants d'équipements physiques/numériques que la personne concernée a utilisés pour se connecter aux systèmes de l'OEB : nom d'hôte et adaptateur réseau du poste de travail, adresse MAC, version du système d'exploitation
- informations de navigation : type de navigateur, URL, agent utilisateur du navigateur, date et heure de navigation, adresse IP, catégorie, historique du site web, historique des interactions réseau
- informations relatives aux appels téléphoniques : numéro de l'appelant, numéro appelé, date et heure, durée, historique des interactions
- données d'interaction téléphoniques : métadonnées de session téléphonique
- données associées au ticket

3. Qui est responsable du traitement des données ?

Les données à caractère personnel de Splunk sont traitées sous la responsabilité de la direction principale CIO/BIT 4.6, agissant en qualité de responsable délégué du traitement de l'OEB.

4. Qui a accès à vos données à caractère personnel et à qui sont-elles communiquées ?

Seuls les destinataires des départements BIT 4.6.2.3 Sécurité de l'information et 4.6.3.8 Gestion réseau et centre de données ont accès aux données à caractère personnel de Splunk, pour les opérations de traitement indispensables.

Splunk est exclusivement utilisé en soutien des cas d'utilisation de sécurité par le département BIT 4.6.2.3 Sécurité de l'information et des cas d'utilisation liés au réseau par le département BIT 4.6.3.8 Gestion réseau et centre de données, conformément au principe du "besoin de savoir".

Des sous-traitants externes peuvent à l'occasion traiter des données Splunk à caractère personnel (et peuvent notamment avoir accès à ces dernières) lors de la prestation de services de maintenance du logiciel Splunk.

5. Comment les données vous concernant sont-elles protégées et préservées ?

L'OEB prend les mesures techniques et organisationnelles nécessaires pour préserver les données à caractère personnel vous concernant et les protéger contre la destruction, la perte ou la modification accidentelles ou illicites ainsi que contre la communication ou l'accès non autorisés.

L'ensemble des données à caractère personnel entrant dans le cadre de la présente opération de traitement est conservé dans une application informatique interne sécurisée, conformément au cadre de la politique de sécurité de l'information de l'OEB.

Sécurité physique : des mesures de contrôle de l'accès physique sont mises en œuvre dans les locaux de l'OEB ; des mesures supplémentaires de contrôle d'accès sont mises en œuvre dans les centres de données de l'OEB au Luxembourg et à Munich.

Sécurité logique : renforcement de la sécurité des systèmes, équipements et réseaux.

Contrôle de l'accès : contrôle de l'accès aux systèmes et au réseau en fonction du rôle, en conformité avec les principes du "besoin de savoir" et du "moindre privilège" ; séparation des rôles d'administrateur et d'utilisateur ; réduction au minimum des rôles d'administrateur.

L'accès à Splunk dépend du rôle. Des groupes Active Directory régissent les rôles affectés aux utilisateurs, qui définissent les restrictions relatives au type d'informations auquel l'utilisateur peut accéder dans Splunk. Des niveaux d'accès appropriés sont accordés à titre individuel uniquement aux destinataires mentionnés ci-dessus.

Authentification de l'utilisateur : tous les postes de travail et serveurs requièrent une ouverture de session ; les appareils mobiles requièrent une ouverture de session dans l'enclave de l'OEB ; les comptes privilégiés requièrent une authentification supplémentaire et plus stricte. Toutes les requêtes réalisées à l'aide de Splunk sont soumises par des utilisateurs authentifiés. L'authentification est basée sur les systèmes Active Directory de l'OEB, afin de garantir que la gestion normale du cycle de vie des comptes est mise en œuvre (p. ex. : désactivation des comptes appartenant à des personnes ne faisant plus partie du personnel).

Journalisation : Splunk conserve un journal d'audit complet des requêtes d'utilisateurs et des autres activités. Ces informations, comme toute autre information disponible dans Splunk, sont "en ajout uniquement" ("append-only"), ce qui signifie qu'une fois saisies, elles ne peuvent être modifiées ou supprimées de manière non détectable.

6. Comment pouvez-vous accéder à vos données, les rectifier et les recevoir, en demander l'effacement, limiter leur traitement ou vous opposer à leur traitement ? Vos droits peuvent-ils être restreints ?

Vous avez le droit d'accéder à vos données à caractère personnel, de les rectifier et de les recevoir, de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, de les effacer, ainsi que de limiter leur traitement ou de vous opposer à celui-ci (articles 18 à 24 RRPD).

Si vous souhaitez exercer l'un de ces droits, veuillez adresser une demande écrite en ce sens au responsable délégué du traitement à l'adresse suivante : DP_BIT@epo.org. Afin de nous permettre de répondre plus rapidement et précisément, vous devez toujours assortir votre demande de certaines informations préliminaires. Nous vous encourageons par conséquent à remplir ce formulaire (pour les externes) ou ce formulaire (pour les internes) et à le transmettre avec votre demande.

Nous répondrons à votre demande sans tarder, et dans tous les cas dans un délai d'un mois à compter de la réception de votre demande. Toutefois, conformément à l'article 15(2) RRPD, ce délai peut être prolongé de deux mois supplémentaires si nécessaire, compte tenu de la complexité et du nombre de demandes reçues. Toute prorogation de délai vous sera notifiée.

7. Sur quelle base juridique est fondé le traitement de vos données ?

Les données à caractère personnel sont traitées en vertu de l'article 5a) RRPD : le traitement est nécessaire à l'accomplissement d'une tâche relevant des activités officielles de l'Organisation européenne des brevets ou de l'exercice légitime de l'autorité publique dont est investi le responsable du traitement, ce qui comprend le traitement nécessaire à la gestion et au fonctionnement de l'Office.

Les données à caractère personnel sont traitées sur la base des instruments juridiques suivants : article 7 "Surveillance, contrôles, audits et suite de la procédure" de la Circulaire nº 382 (29 mars 2017) Directives relatives à la sécurité de l'information à l'OEB.

8. Combien de temps conservons-nous vos données à caractère personnel ?

Les données à caractère personnel de Splunk sont conservées uniquement pendant une durée n'excédant pas celle nécessaire à la finalité de leur traitement.

Les données stockées dans Splunk sur site sont soumises à la politique de sauvegarde, d'archivage et de conservation applicable aux serveurs sur site.

Les fichiers journaux Splunk sont enregistrés automatiquement et conservés pour une durée convenue en fonction du type d'information et du système auxquels ils se rapportent. Les données d'alerte/d'incident de Microsoft Defender pour point de terminaison sont conservées pendant 12 mois dans Splunk. Les autres données sont conservées dans Splunk pour une durée maximale de 18 mois, après quoi elles sont automatiquement effacées. Les données sont conservées dans un système de sauvegarde pendant 60 jours après leur expiration dans le système Splunk, après quoi elles ne sont plus disponibles. Cela signifie que la conservation des données de Splunk ne dépasse jamais 20 mois.

En cas de recours formel/contentieux, toutes les données détenues au moment où le recours formel/contentieux est engagé seront conservées jusqu'à la clôture de la procédure.

9. Personnes à contacter et coordonnées

Si vous avez des questions sur le traitement de vos données à caractère personnel, veuillez vous adresser au responsable délégué du traitement à l'adresse suivante : DP_BIT@epo.org si vous êtes un agent de l'OEB, ou DPOexternalusers@epo.org si vous êtes une personne concernée externe.

Notre responsable de la protection des données peut également être contacté à l'adresse suivante dpo@epo.org (pour les internes) et à l'adresse suivante DPOexternalusers@epo.org (pour les externes).

Réexamen et exercice des voies de recours

Si vous considérez que le traitement porte atteinte à vos droits en tant que personne concernée, vous avez le droit de demander un réexamen par le responsable délégué du traitement en vertu de l'article 49 RRPD et le droit d'exercer des voies de recours en vertu de l'article 50 RRPD.