# Rundschreiben Nr. 421

EPA-Richtlinie zur Videoüberwachung

**Artikel 1 – Einführung**

(1) Das exponentielle Wachstum der Technologien, in denen personenbezogene Daten verarbeitet werden, darunter Videoüberwachungssysteme, gibt Anlass zu Besorgnis hinsichtlich der Grundrechte und Grundfreiheiten betroffener Personen, insbesondere seit intelligente Videoanalysetools Teil dieser Technologien sind. Trotz der echten Schutz- und Sicherheitszwecke, denen diese Systeme dienen sollen, verdienen die Auswirkungen, die sie auf die Privatsphäre und die Rechte betroffener Personen haben, besondere Aufmerksamkeit.

(2) Der Einsatz der Videoüberwachung gemäß der hier dargelegten Richtlinie zur Videoüberwachung (nachstehend "diese Richtlinie") ist Teil der Richtlinien für die physische Sicherheit (Rundschreiben Nr. 381). Diese Richtlinie soll den Rahmen und die Leitlinien schaffen, nach denen das Videoüberwachungssystem (nachstehend "VÜS") im EPA entwickelt, eingesetzt und genutzt wird. Sie beschreibt das VÜS und die Sicherheitsmaßnahmen, die das EPA getroffen hat, um den Schutz der personenbezogenen Daten, der Privatsphäre sowie sonstiger Grundrechte und berechtigter Interessen der durch das VÜS betroffenen Personen zu gewährleisten und sicherzustellen, dass das VÜS dem für den Schutz personenbezogener Daten im EPA geltenden Rechtsrahmen andauernd entspricht, der insbesondere in den Artikeln 1b und 32a des Statuts und den dazugehörigen Vorschriften verankert ist.

(3) Diese Richtlinie wird von der EPA-Abteilung, die das VÜS bedient, unter der Verantwortung des delegierten Verantwortlichen alle zwei Jahre überprüft, wobei die erste Überprüfung Ende 2024 stattfindet. Dabei wird das EPA prüfen, ob das VÜS weiterhin notwendig ist und seinem erklärten Zweck dient, ob der Anwendungsbereich angemessen ist und welche Alternativen es gibt. Bei der Überprüfung wird legislativen Entwicklungen Rechnung getragen, um sicherzustellen, dass diese Richtlinie weiter dem geltenden Rechtsrahmen entspricht. Kopien der regelmäßigen Überprüfungsberichte werden im Intranet und/oder auf der Website des EPA bereitgestellt.

(4) Mit der Einführung der neuen Datenschutzvorschriften (nachstehend "DSV") und dieser Richtlinie gleicht das EPA seine Politik an die höchsten internationalen Standards und optimalen Praktiken an, die in anderen internationalen Organisationen sowie angesichts der Empfehlungen des Europäischen Datenschutzbeauftragten und des Europäischen Datenschutzausschusses in EU-Einrichtungen, -Organen und -Agenturen befolgt werden.

**Artikel 2 – Anwendungsbereich**

Diese Richtlinie gilt für alle natürlichen Personen (nachstehend "betroffene Personen"), die ab dem Zeitpunkt, ab dem sie sich in unmittelbarer Nähe von EPA-Gebäuden befinden bzw. diese betreten, direkt oder indirekt identifiziert werden können und deren personenbezogene Daten vom VÜS verarbeitet werden. Dazu gehören auch die Kameras, die für die automatische Nummernschilderkennung (nachstehend "ANPR") verwendet und an einigen Eingängen zu EPA-Parkflächen eingesetzt werden, um Bediensteten und Besuchern mit ihren Fahrzeugen den Zugang zu und das Nutzen der EPA-Parkflächen zu ermöglichen.

**Artikel 3 – Grundsätze**

Im Einklang mit dem Datenschutzrahmen des EPA beruht diese Richtlinie auf den folgenden wesentlichen Grundsätzen:

a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Die Nutzung des VÜS ist für die korrekte Verwaltung und die Arbeitsweise des EPA erforderlich. Die Nutzung des VÜS ist nach Artikel 5 a) und e) DSV rechtmäßig. Eine weitere Rechtsgrundlage findet sich in Rundschreiben Nr. 381, wonach das EPA die darin definierten Sicherheitsgrundsätze umzusetzen hat und in dem festgelegt ist, in welchen Bereichen Videoüberwachung eingesetzt werden kann (Artikel 7), um die EPA-Bediensteten und sich in den Räumlichkeiten des EPA befindende Dritte sowie die Vermögenswerte der Europäischen Patentorganisation zu schützen.

Gemäß Artikel 20 des Protokolls über die Vorrechte und Immunitäten der Europäischen Patentorganisation ist die Organisation verpflichtet, mit den zuständigen Behörden der Vertragsstaaten zusammenzuarbeiten, um u. a. die Einhaltung der Vorschriften über Sicherheit und Ordnung zu gewährleisten, was Sicherheitsangelegenheiten umfasst. Diese Pflicht bleibt von dieser Richtlinie unberührt.

Personenbezogene Daten können auch als rechtmäßig verarbeitet angesehen werden, wenn sie dazu verwendet werden, die lebenswichtigen Interessen von betroffenen Personen oder anderen natürlichen Personen zu schützen.

Informationen über die Existenz des VÜS werden der Öffentlichkeit zugänglich gemacht. Sie werden in einem mehrschichtigen Ansatz durch Schilder und die Veröffentlichung dieser Richtlinie bereitgestellt.

b) Zweckbindung

Die Verarbeitungsvorgänge sollen es ermöglichen, Fragen der Sicherheit und Betriebssicherheit effizient anzugehen, Identitäten zu verifizieren und den Zugang zu EPA-Gebäuden und Informationsverarbeitungseinrichtungen (z. B. EPA-Rechenzentrum) zu überwachen.

Personenbezogene Daten, die für die Erreichung der beabsichtigten Zwecke nicht relevant oder notwendig sind, werden nicht erhoben.

Die Verarbeitung personenbezogener Daten zu anderen Zwecken ist weiterhin möglich, sofern diese mit den primären Zwecken vereinbar sind. In solchen Fällen führt der delegierte Verantwortliche vor dem Verarbeitungsvorgang eine Vereinbarkeitsprüfung durch, um den Grad der Vereinbarkeit des Verarbeitungsvorgangs zu ermitteln. Das Ergebnis dieser Prüfung bestimmt, ob die zusätzlichen Zwecke explizit oder implizit abgedeckt sind, und liefert die erforderlichen Leitlinien für die Feststellung, ob die Verarbeitung fair ist und erfolgen kann.

Das System wird genutzt, um den Bereich um unsere Gebäude und den Zugang zu den Gebäuden und zu Bereichen, in denen sensible Informationen verarbeitet oder gespeichert werden, zu überwachen, was den Schutz des geistigen Eigentums und sensibler Informationen verbessert.

Bei Vorfällen wie Eindringen, Diebstahl oder Evakuierung wird das System auch zur Unterstützung der betrieblichen Sicherheitsaktivitäten des externen Sicherheitsdienstleisters genutzt, der für die Ausführung der zugehörigen Prozesse verantwortlich ist.

Der delegierte Verantwortliche stellt sicher, dass personenbezogene Daten für die festgelegten, eindeutigen und rechtmäßigen Zwecke, für die sie erhoben wurden, verarbeitet werden (Zweckbestimmung), und verhindert jede Weiterverarbeitung, die mit diesen Zwecken unvereinbar sein könnte (vereinbare Nutzung). Werden die Daten für mehrere Zwecke verarbeitet, wird jeder von ihnen ausdrücklich erwähnt.

c) Datenminimierung

Das VÜS ist so konzipiert, dass nur personenbezogene Daten erfasst werden, die dem Zweck angemessen, erheblich und auf die beabsichtigten Zwecke beschränkt sind.

Wenn Überwachungskameras oder andere Zusatzartikel mit Geräten zum Empfangen oder Senden von Tönen ausgestattet sind, werden diese deaktiviert oder ausgeschaltet. Dies gilt nicht für Intercom-Kameras, bei denen das Sende-/Empfangsgerät verwendet wird, um die Kommunikation mit der betroffenen Person zu erleichtern, aber in diesen Fällen wird der gesendete bzw. empfangene Ton nicht aufgezeichnet. Ähnlich ist die Auswahl der technischen Lösungen auf Systeme beschränkt, die nur die benötigten Funktionalitäten bieten und bei denen nicht benötigte Funktionen deaktiviert werden.

Bei der Auswahl technischer Lösungen berücksichtigt der delegierte Verantwortliche zunächst datenschutzfreundliche Systeme, die das Verwürfeln oder Maskieren von Bereichen ermöglichen würden, die für die beabsichtigten Überwachungszwecke nicht relevant sind oder bei denen Datenschutzbedenken bestehen.

Das VÜS verarbeitet die folgenden personenbezogenen Daten:

- Vor- und Nachname sowie Personalnummer von Nutzern mit Zugriff auf die Software-Anwendungen, die für die Überwachung der Videoüberwachungskameras verwendet werden
- Bilder von Bediensteten, Besuchern und Auftragnehmern sowie deren Fahrzeugen, die das EPA-Gelände betreten, einschließlich Datums- und Zeitstempel der Bilder

- Bilder von Bediensteten, Besuchern und Auftragnehmern, die die verschiedenen Sicherheitszonen des EPA betreten oder verlassen oder sich in den Hochsicherheits- oder Kernversorgungszonen befinden.
- Kfz-Kennzeichen von Bediensteten und Besuchern, die in EPA-Parkflächen einfahren
- Metadaten der vom System erfassten Bilder (z. B. Bewegung, Richtung, Zeit, Geschwindigkeit)

In die Bilder eingebettete Metadaten werden verwendet, um Sicherheitsverletzungen wie zurückgelassene Gegenstände und Bewegungen zu identifizieren, die verdächtig oder unstet sind oder in eine ungewöhnliche Richtung gehen und damit Alarm auslösen. Sie optimieren die Nutzung des Systems, indem sie die Zeit reduzieren, die die Beschäftigten des Sicherheitsdienstes für das Betrachten der Bilder benötigen. Metadaten ermöglichen außerdem eine schnellere Suche in gespeicherten Bildern, ohne dass viel Zeit darauf verwendet werden muss.

Das VÜS

- sammelt keine besonderen Kategorien personenbezogener Daten,
- nutzt keine biometrischen Daten,
- zeichnet keine Gespräche auf und
- zeichnet keine Bilder von Personen in Bereichen auf, in denen erhöhte Erwartungen an die Privatsphäre gestellt werden.

Der delegierte Verantwortliche konsultiert die Datenschutzbeauftragte zu Änderungen der Kategorien der erhobenen personenbezogenen Daten oder der vom VÜS überwachten Bereiche, bevor diese Änderungen umgesetzt werden.

**Überwachte Bereiche**

Das EPA hat ein Sicherheitszonenmodell eingeführt, in dem Bereiche auf der Grundlage der Sicherheitsrisiken, denen sie ausgesetzt sind, und der von ihnen unterstützten Sicherheitsprozesse abgegrenzt wurden. Es besteht aus fünf eindeutigen Sicherheitszonen, von der niedrigsten Sicherheitsstufe oder Zone Null, die öffentlich zugängliche Bereiche umfasst, bis zur höchsten Sicherheitsstufe oder Zone vier, in der vertrauliche Daten verarbeitet oder gespeichert werden. Der Einsatz von Videoüberwachungskameras in diesen Zonen basiert auf regelmäßigen Risikobewertungen durch das EPA, die im Verzeichnis der Verarbeitungstätigkeiten für das VÜS beschrieben sind.

Marke, Typ, Funktion, Standort und Zweck der einzelnen Videoüberwachungskameras sind in einem vertraulichen Dokument enthalten und können von der Datenschutzbeauftragten und dem delegierten Verantwortlichen eingesehen werden.

ANPR-Kameras werden ebenfalls eingesetzt und erleichtern Bediensteten mit ihren Fahrzeugen den Zugang zu den Parkplätzen auf dem Gelände des EPA.

Bereiche mit erhöhten Erwartungen an die Privatsphäre wie Büros, Freizeitbereiche, Kantinen, Bars, Cafeterien, Toiletten, Duschen und Umkleidekabinen werden nicht überwacht.

In allen Fällen, in denen der Verarbeitungsvorgang mit einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen verbunden sein dürfte, wird eine Datenschutz-Folgenanalyse durchgeführt.

d) Richtigkeit

Der delegierte Verantwortliche stellt sicher, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind und dass alle unrichtigen Daten im Hinblick auf die Zwecke, für die sie verarbeitet werden, unverzüglich gelöscht oder berichtigt werden.

Dafür legt er die erforderlichen Standardarbeitsanweisungen (nachstehend SOPs) fest, die von der Datenschutzbeauftragten eingesehen werden können. In den SOPs sind die Maßnahmen definiert, die ergriffen werden, um sicherzustellen, dass die im VÜS verarbeiteten oder gespeicherten personenbezogenen Daten regelmäßig geprüft werden, damit gewährleistet ist, dass die erhobenen Daten richtig und auf dem neuesten Stand sind. Ferner ist darin das Verfahren zur Berichtigung veralteter oder unrichtiger Daten definiert, die vom delegierten Verantwortlichen festgestellt oder von der betroffenen Person gemeldet werden (Art. 19 DSV: Recht auf Berichtigung, und Art. 20 DSV: Recht auf Löschung).

Das VÜS ist mit dem EPA-Zeitserver verbunden, der die Protokolle des Zugriffskontroll- und des Sicherheitsmanagementsystems synchronisiert und so sicherstellt, dass alle von einem der beiden aufgezeichneten Ereignisse korrekt gemeldet werden.

e) Speicherbegrenzung

Personenbezogene Daten werden gelöscht, sobald sie für die Zwecke, für die sie erhoben wurden, nicht mehr benötigt werden.

Unter Berücksichtigung der Rechtsgrundlage und der Zwecke, die für die Verarbeitung personenbezogener Daten mittels des VÜS festgelegt wurden, wird die maximale Aufbewahrungsdauer für die erfassten Bilder auf sieben Tage festgelegt[1]; danach werden die Bilder automatisch gelöscht. Diese Aufbewahrungsdauer kann für Sicherungskopien von Bildern im Zusammenhang mit identifizierten Vorfällen verlängert werden, wenn das Bildmaterial Teil der Beweismittel zur Stützung von Ermittlungen, Beschwerden, Rechtsstreitigkeiten oder Ansprüchen wird. Sie kann solange verlängert werden, bis die Ermittlungen, Beschwerden, Rechtsstreitigkeiten oder Ansprüche beigelegt sind.

f) Integrität und Vertraulichkeit

Der delegierte Verantwortliche stellt sicher, dass alle geeigneten technischen und organisatorischen Maßnahmen zur Wahrung der Sicherheit und Vertraulichkeit personenbezogener Daten getroffen wurden, einschließlich Schutz vor unbeabsichtigtem Verlust bzw. unbeabsichtigter Beeinträchtigung, Zerstörung, Schädigung oder Weitergabe. Die Sicherheitsmaßnahmen werden von Fall zu Fall analysiert, regelmäßig überprüft und angepasst.

Gemäß Punkt 6.9 der Allgemeinen Vertragsbedingungen und gegebenenfalls gemäß den Bedingungen, die in den von den Unternehmen unterzeichneten Datenverarbeitungsvereinbarungen vereinbart wurden, gewährleisten alle Auftragnehmer, die personenbezogene Daten verarbeiten, dass die Daten im Einklang mit den geltenden Gesetzen und

[1] Die Aufbewahrungsdauer für andere Kategorien von Daten ist im Verzeichnis der Verarbeitungstätigkeiten für das VÜS angegeben.

Vorschriften, insbesondere den DSV, verarbeitet werden. Auch interne Bedienstete sind an die DSV gebunden.

Der delegierte Verantwortliche ist für die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen verantwortlich, die die Integrität und Vertraulichkeit der im VÜS verarbeiteten oder gespeicherten personenbezogenen Daten gewährleisten. Diese Maßnahmen stehen in einem angemessenen Verhältnis zum Risiko von Zerstörung, Veränderung, unbefugtem Zugriff oder unbefugter Offenlegung, das das VÜS für die Rechte und Freiheiten der betroffenen Personen mit sich bringt.

**Schutzmaßnahmen**

Die im VÜS verarbeiteten oder gespeicherten personenbezogenen Daten werden so geschützt, dass die Trennung von Funktionen möglich ist und der Zugriff auf personenbezogene Daten auf der Grundlage von Rollen und Funktionen eingeschränkt wird.

Soweit technisch möglich implementiert der delegierte Verantwortliche die nach ISO 27001 geltenden Kontrollen, insbesondere die Kontrollen für mobile Geräte und Telearbeit, Personalsicherheit, Anlagenverwaltung, Umgang mit Medien, Zugriffskontrolle, Kryptographie, sichere Bereiche und Gerätesicherheit.

Es werden regelmäßige interne Prüfungen (Schwachstellentests) durchgeführt, um die Integrität, Vertraulichkeit und Verfügbarkeit des Systems und seiner Komponenten sowie den Erfüllungsgrad in Bezug auf die vorstehend genannten Kontrollen zu überprüfen.

Der Zugriff auf das VÜS erfordert die Authentifizierung über Tools aus dem Bereich Business Information Technology (Passwort/Active Directory) sowie ein zusätzliches Passwort für die Anwendung.[2]

Alle aufgezeichneten Bilder werden verschlüsselt. Alle personenbezogenen Daten werden in sicheren IT-Anwendungen gemäß den Sicherheitsstandards des EPA gespeichert. Dazu gehören:

- Nutzerauthentifizierung: Alle Workstations und Server benötigen die Standardanmeldung, mobile Geräte benötigen eine Anmeldung für den EPA-internen Bereich, privilegierte Konten benötigen eine zusätzliche und strengere Authentifizierung.
- Zugriffskontrolle (z. B. rollenabhängige Zugriffskontrolle auf die Systeme und das Netzwerk, Bedarfsorientiertheit und Least-Privilege-Prinzip): Trennung in Administrator- und Nutzerrollen, Nutzer haben eine minimale Berechtigung, allgemeine Administratorrollen werden auf ein Minimum beschränkt
- Sicherheitshärtung von Systemen, Geräten und Netzwerk: 802.1X für den Netzwerkzugang, Verschlüsselung von Endgeräten, Virenschutzsoftware auf allen Geräten
- physischer Schutz: EPA-Zugangskontrollen, zusätzliche Zugangskontrollen für das Rechenzentrum, Regeln für das Abschließen von Büros
- Übertragungs- und Eingabekontrollen (z. B. Audit-Protokollierung, System- und Netzwerküberwachung): Sicherheitsüberwachung mit spezieller Software, die maschinengenerierte Daten analysiert, um Bedrohungen zu erkennen

[2] In Den Haag umgesetzt; soll in naher Zukunft schrittweise auf die anderen EPA-Dienstorte ausgeweitet werden.

- Reaktion auf sicherheitsrelevante Vorfälle: Rund-um-die-Uhr-Überwachung auf Vorfälle, Sicherheitsexperte in Bereitschaft

**Zugriff auf personenbezogene Daten**

Einer begrenzten Zahl von Personen, die diese Informationen benötigen und die regelmäßig im Datenschutz geschult werden, wird der Zugriff auf personenbezogene Daten oder auf die Systeme gewährt, in denen die Daten verarbeitet oder gespeichert werden. Die Liste der Personen mit Zugriff ist im vertraulichen Dokument "Liste der Personen, die im Rahmen ihrer Zugriffsrechte Zugriff auf das VÜS haben" enthalten.

Der Zugriff einzelner Personen basiert jeweils auf ihren Rollen und Zuständigkeiten und ist stets zeitlich und sachlich auf das Minimum beschränkt, das für die Erfüllung ihrer spezifischen Aufgaben erforderlich ist (z. B. Sicherheit, Wartung, Systemadministration).

Das Sicherheitspersonal, das für den Schutz der EPA-Gebäude zuständig ist, erhält Zugriff auf die Aufzeichnungen der letzten 60 Minuten. Zweck dieses Zugriffs ist die Verarbeitung von Alarmen und die Unterstützung bei Notfällen in diesem begrenzten Zeitrahmen.

Die Liste der Personen mit Zugriff auf personenbezogene Daten oder Systeme, in denen die Daten verarbeitet oder gespeichert werden, wird regelmäßig überprüft und aktualisiert. Verfahren für das Gewähren, Ändern und Widerrufen von Zugriffsrechten sind jederzeit verfügbar.

Der Zugriff auf im System gespeicherte personenbezogene Daten (z. B. zur Beurteilung eines Vorfalls) erfordert die vorherige Genehmigung des delegierten Verantwortlichen, der die Datenschutzbeauftragte konsultieren kann. Alle Einzelheiten zum Zugriff auf personenbezogene Daten sind im Dokument "Protokolle über den Zugriff auf personenbezogene Daten" festgehalten.

**Offenlegung personenbezogener Daten**

Die im VÜS verarbeiteten oder gespeicherten personenbezogenen Daten werden nur intern von der Abteilung des EPA, die das VÜS bedient, und von Beschäftigten des externen Sicherheitsdienstleisters genutzt, um sie bei der Erfüllung ihrer Aufgaben zu unterstützen.

Andere Personen haben das Recht, beim delegierten Verantwortlichen den Zugriff auf ihre personenbezogenen Daten zu beantragen; dieser kann dazu die Datenschutzbeauftragte konsultieren.

Im Falle eines höchst gefährlichen Fahrverhaltens kann der delegierte Verantwortliche den Sicherheitsexperten des EPA zwecks Analyse und fachkundiger Beratung Zugriff auf die Videoaufnahmen des Vorfalls gewähren und gegebenenfalls die Datenschutzbeauftragte um Rat fragen.

Bei Unfällen oder Vorfällen, die zu Versicherungsansprüchen führen, kann der delegierte Verantwortliche auch dem Unternehmen, das den Anspruch bearbeitet, Zugriff auf das relevante Videomaterial gewähren, sofern alle einschlägigen Datenschutzvorschriften betreffend eine solche Offenlegung eingehalten werden.

Der delegierte Verantwortliche führt ein genaues Register, in dem er die Offenlegung dokumentiert, einschließlich Rechtsgrundlage, Datum und Uhrzeit, Art der offengelegten personenbezogenen Daten und Empfänger.

**Artikel 4 – Individuelle Rechte**
**Recht auf Unterrichtung**

(1) Einzelpersonen haben das Recht, vom Verantwortlichen eine Bestätigung darüber zu erhalten, ob ihre personenbezogenen Daten verarbeitet werden. Betroffene Personen erhalten Informationen in Einklang mit Artikel 16 DSV. Informationen über die Existenz des VÜS werden der Öffentlichkeit in einem mehrschichtigen Ansatz wie folgt bereitgestellt.

(2) Informationsschilder bilden die erste Schicht. Diese Schilder in einer ihrem Standort angemessenen Größe sind deutlich sichtbar und lesbar. Sie enthalten Informationen zum delegierten Verantwortlichen, zum Zweck der Verarbeitungsvorgänge und Kontaktdaten. Angegeben ist ferner, wo relevante zusätzliche Informationen wie z. B. die Rechte betroffener Personen zu finden sind. Ein Link oder ein QR-Code verweisen auf den Ort, wo betroffene Personen die Informationen leicht finden können.

(3) Die zweite Schicht ist diese Richtlinie, die über den Link auf den Warnschildern zugänglich und in Papierform in den Empfangsbereichen der EPA-Gebäude erhältlich ist.

(4) Es ist nicht notwendig, Kamerapositionen öffentlich zu machen, solange die betroffenen Personen leicht erkennen können, dass sie überwachte Bereiche betreten.

**Weitere Rechte betroffener Personen**

(1) Vom VÜS erfasste Personen haben das Recht, auf das Bildmaterial zuzugreifen, das Recht auf Berichtigung, Widerspruch und Löschung sowie das Recht auf Beschränkung der Verarbeitung.

(2) Betroffene Personen können alle vorstehend genannten Rechte ausüben, indem sie beim delegierten Verantwortlichen einen schriftlichen Antrag stellen, der innerhalb eines Monats ab Eingang des Antrags darauf antworten wird.

(3) Der delegierte Verantwortliche bearbeitet Anträge auf Zugriff sowie auf Bereitstellung, Löschung, Korrektur, Berichtigung oder Vervollständigung personenbezogener Daten baldmöglichst und innerhalb eines Monats nach Eingang des Antrags.

(4) Der delegierte Verantwortliche kann die Bereitstellung der Informationen verweigern, wenn nachgewiesen werden kann, dass der Antrag offenkundig unbegründet oder exzessiv ist.

**Artikel 5 – Fortbildung**

(1) Die Datenschutzbeauftragte fördert regelmäßige Schulungsprogramme zum Datenschutz und sensibilisiert die an den Verarbeitungsvorgängen beteiligten EPA-Bediensteten für dieses Thema. Die Vertragsmanager der Auftragnehmer, die an den Verarbeitungsvorgängen beteiligt sind, stellen sicher, dass die Beschäftigten des Auftragnehmers entsprechend geschult sind und diese Richtlinie einhalten.

(2) Die Schulung ist für alle Bediensteten, die Zugriff auf personenbezogenen Daten – ob live oder aufgezeichnet – haben, obligatorisch und umfasst mindestens die Risiken, die Verarbeitungsvorgänge für personenbezogene Daten mit sich bringen, unter besonderer Berücksichtigung der Vorsichtsmaßnahmen, die bei der Verarbeitung von personenbezogenen Daten aus besonderen Kategorien zu treffen sind. Es werden die folgenden Punkte behandelt:

- die EPA-Richtlinie für die Aufzeichnung und Aufbewahrung von Informationen
- sicherer Umgang mit Informationen
- Vorgehensweise, wenn eine Informationsanfrage, beispielsweise von der Polizei, eingeht
- Zeichen, dass es sich um einen Antrag einer betroffenen Person handelt, und Vorgehensweise, wenn ein solcher eingeht

**Artikel 6 – Unterlagen, die vom delegierten Verantwortlichen aufzubewahren sind (vertraulich)**

- Karte mit den Standorten aller Videoüberwachungskameras
- Schwachstellentest mit Ergebnissen und Aktionsplan sowie Bearbeitungsstand
- Datenschutz-Folgenanalyse
- Protokolle über Datenschutzschulungen
- Protokolle über den Zugriff auf personenbezogene Daten
- Liste der Personen, die im Rahmen ihrer Zugriffsrechte Zugriff auf das VÜS haben
- Standardarbeitsanweisung (SOP) für das Gewähren, Ändern und Widerrufen von physischen und logischen Zugriffsrechten
- SOP für die Überprüfung der Richtigkeit verarbeiteter oder gespeicherter personenbezogener Daten
- Verträge mit Sicherheitsdienstleistern
- Sicherheitsmodell des EPA einschließlich Sicherheitszonen

**Artikel 7 – Kontaktdaten**

Einzelpersonen können sich bei Fragen an den delegierten Verantwortlichen des EPA wenden unter dpl.pd44@epo.org.

Die Datenschutzbeauftragte ist unter dpo@epo.org zu erreichen.

## Anlagen

- Datenschutzvorschriften
- Rundschreiben Nr. 380
- Rundschreiben Nr. 381

München, den 16.12.2022

Präsident des Europäischen Patentamts

António Campinos