Circulaire n° 421

Politique de vidéosurveillance de l'OEB

Article premier – Introduction

(1) La croissance exponentielle des technologies dans lesquelles des données à caractère personnel sont traitées, dont les systèmes de vidéosurveillance, fait naître des inquiétudes quant aux droits fondamentaux et aux libertés des personnes concernées, en particulier depuis que des outils intelligents d'analyse vidéo ont été intégrés à ces systèmes. Malgré les finalités réelles de sûreté et de sécurité que ces systèmes visent à servir, leur incidence sur la vie privée et les droits des personnes concernées mérite une attention particulière.

(2) L'utilisation de la vidéosurveillance conformément à la politique de vidéosurveillance définie ici (ci-après "la présente politique") fait partie des Directives relatives à la sécurité physique (circulaire n° 381). La présente politique vise à fournir le cadre et les principes directeurs selon lesquels le système de vidéosurveillance (ci-après dénommé "le SVS") de l'OEB est conçu, déployé et utilisé. Elle décrit le SVS et les garde-fous mis en place par l'OEB pour assurer la protection des données à caractère personnel, de la vie privée et des autres droits fondamentaux et intérêts légitimes des personnes affectées par le SVS et pour garantir que le SVS soit en permanence conforme au cadre juridique applicable à la protection des données à caractère personnel à l'OEB, tel qu'il est en particulier défini dans les articles 1ter et 32bis du statut et les règlements d'application y afférents.

(3) La présente politique sera révisée par le département de l'OEB qui exploite le SVS sous la responsabilité du responsable délégué du traitement, tous les deux ans, la première révision devant être effectuée d'ici la fin 2024. Lors de ces révisions, l'OEB examinera si le SVS est nécessaire, s'il continue de servir la finalité prévue, quelle est sa portée et quelles autres solutions existent. La révision tiendra compte de l'évolution de la législation afin de veiller à ce que la présente politique soit encore conforme au cadre législatif applicable. Des copies des rapports relatifs aux révisions périodiques seront disponibles sur l'Intranet et/ou le site Internet de l'OEB.

(4) Avec l'introduction du nouveau règlement relatif à la protection des données (ci-après "le RRPD") et de la présente politique, l'OEB s'aligne sur les normes internationales les plus rigoureuses et les meilleures pratiques suivies dans d'autres organisations internationales et dans les institutions, organes et agences de l'UE, à la lumière des recommandations du contrôleur européen de la protection des données et du Conseil européen de la protection des données.

Article 2 – Champ d'application

La présente politique s'applique à toutes les personnes physiques (ci-après dénommées "personnes concernées") qui, se trouvant à proximité des locaux de l'OEB ou y pénétrant, peuvent être identifiées directement ou indirectement, et dont les données personnelles sont donc traitées par le SVS à partir de ce moment. Ce système inclut les caméras utilisées pour la reconnaissance automatique de la plaque d'immatriculation (ci-après "RAPI") qui sont en service à certaines entrées de parkings de l'OEB pour autoriser les véhicules des agents et des visiteurs à entrer et à utiliser les parcs de stationnement de l'OEB.

Article 3 – Principes

Conformément au cadre de protection des données de l'OEB, la présente politique repose sur les principes clés ci-après.

(a) Licéité, loyauté et transparence

L'utilisation du SVS est nécessaire pour assurer la gestion et le fonctionnement corrects de l'OEB. L'utilisation du SVS est licite conformément à l'article 5(a) et à l'article 5(e) du RRPD. En outre, elle trouve son fondement juridique dans la circulaire n° 381, qui exige de l'OEB qu'il mette en œuvre les principes de sécurité qui y sont définis et précise quelles zones peuvent faire l'objet d'une vidéosurveillance (article 7) afin de protéger les agents de l'OEB et les tiers dans les bâtiments de l'OEB ainsi que les actifs de l'Organisation.

Aux termes de l'article 20 du Protocole sur les privilèges et immunités de l'Organisation européenne des brevets, l'Organisation a l'obligation de coopérer avec les autorités compétentes des États contractants, et notamment d'assurer l'observation des règlements de police, ce qui inclut les questions de sécurité. La présente politique ne déroge pas à cette obligation.

Les données à caractère personnel peuvent également être considérées comme traitées de manière licite lorsqu'elles sont utilisées pour protéger les intérêts vitaux des personnes concernées ou d'une autre personne physique.

Des informations sur l'existence du SVS seront mises à la disposition du public. Ces informations seront fournies selon une approche par niveaux, au moyen de panneaux et par la publication de la présente politique.

(b) Limitation des finalités

Les opérations de traitement ont pour finalité de permettre le traitement efficace des problèmes de sécurité et de sûreté opérationnelle, la vérification des identités et le contrôle des accès aux bâtiments de l'OEB et aux équipements de traitement de l'information (par exemple : centre de données de l'OEB).

Les données personnelles qui ne sont pas pertinentes ou nécessaires à cette fin ne sont pas collectées.

Le traitement de données personnelles à d'autres fins reste possible, à condition que ces autres finalités soient compatibles avec les finalités initiales. En pareil cas, et préalablement à l'opération de traitement, le responsable délégué du traitement procèdera à une évaluation de la compatibilité pour déterminer le degré de compatibilité de l'opération de traitement. Le résultat de l'évaluation déterminera si les finalités supplémentaires sont explicitement ou implicitement couvertes et fournira les directives nécessaires pour déterminer si le traitement est loyal et peut avoir lieu.

Le système est utilisé pour surveiller les abords de nos bâtiments et l'accès aux bâtiments et aux zones où des informations sensibles sont traitées ou stockées, ce qui améliore la protection de la propriété intellectuelle et des informations sensibles.

En cas d'incidents tels qu'une intrusion, un vol ou une évacuation, le système est également utilisé en appui aux activités de sécurité opérationnelle du prestataire de services de sécurité externe qui est responsable de l'exécution des procédures correspondantes.

Le responsable délégué du traitement veille à ce que les données personnelles soient traitées pour les finalités déterminées, explicites et légitimes pour lesquelles elles ont été collectées (détermination de la finalité), ce qui empêche tout traitement ultérieur qui pourrait être incompatible avec ces finalités (utilisation compatible). Si les données sont traitées à des fins multiples, chacune d'entre elles est mentionnée explicitement.

(c) Minimisation des données

Le SVS est conçu pour capter uniquement les données personnelles qui sont adéquates, pertinentes et se limitent aux finalités prévues.

Si des caméras de surveillance ou d'autres appareils auxiliaires sont équipés de dispositifs de réception ou d'émission des sons, ceux-ci sont désactivés ou éteints. Cela ne s'applique pas aux caméras d'interphones où le dispositif audio est utilisé pour faciliter la communication avec la personne concernée, mais dans ce cas, le son émis ou reçu n'est pas enregistré. De même, la sélection des solutions techniques est limitée aux systèmes qui ne fournissent que les fonctionnalités nécessaires, et toutes les fonctions non requises sont désactivées.

Lors de la sélection de solutions techniques, le responsable délégué du traitement privilégiera les systèmes respectueux de la vie privée qui permettraient de brouiller ou de masquer les zones qui ne sont pas pertinentes pour les finalités de surveillance prévues, ou posent des problèmes en matière de protection de la vie privée.

Le SVS traite les données personnelles ci-après :

- nom, prénom et numéro personnel des utilisateurs qui accèdent aux applications logicielles utilisées pour surveiller les caméras de vidéosurveillance
- images des agents, des visiteurs, des fournisseurs et de leurs véhicules qui accèdent aux locaux de l'OEB, y compris date et heure des images
- images des agents, des visiteurs et des fournisseurs qui accèdent aux différentes zones de sécurité de l'OEB ou les quittent, ou qui se trouvent dans les zones ayant un niveau de sécurité élevée ou les zones comportant des équipements essentiels
- numéro d'immatriculation des agents et des visiteurs qui accèdent aux parcs de stationnement de l'OEB

- métadonnées des images captées par le système (mouvement, direction, heure, vitesse, etc.).

Les métadonnées intégrées aux images sont utilisées pour identifier les atteintes à la sécurité que peuvent constituer des objets abandonnés et des déplacements suspects, dans des directions inhabituelles ou irréguliers, ce qui peut déclencher des alarmes. Elles optimisent l'utilisation du système en réduisant le temps nécessaire aux agents de sécurité pour regarder les images. Les métadonnées permettent également des recherches plus rapides dans les images stockées, sans qu'il soit nécessaire d'y passer beaucoup de temps.

Ce que le SVS ne fait pas :

- collecter des catégories particulières de données personnelles
- utiliser des données biométriques
- enregistrer des conversations
- enregistrer des images de personnes dans des zones où les attentes en matière de protection de la vie privée sont plus élevées.

Le responsable délégué du traitement consulte le responsable de la protection des données (ci-après dénommé "le RPD") au sujet de toute modification apportée aux catégories de données personnelles collectées ou aux zones surveillées par le SVS avant la mise en œuvre de ces modifications.

Zones sous surveillance

L'OEB a établi un modèle de zonage de sécurité dans lequel des zones ont été délimitées en fonction des risques de sécurité auxquels elles sont soumises et des procédures de sécurité dont elles font l'objet. Dans ce modèle, il existe cinq zones de sécurité distinctes, allant du niveau de sécurité le plus bas ou de la zone zéro, qui comprend les espaces accessibles au public, au niveau de sécurité le plus élevé ou à la zone quatre, dans laquelle des données confidentielles sont traitées ou stockées. Le déploiement de caméras de surveillance vidéo dans ces zones se fonde sur des évaluations régulières des risques effectuées par l'OEB et dont le détail figure dans le registre des activités de traitement du SVS.

La marque, le type, la fonction, l'emplacement et la finalité de chaque caméra de vidéosurveillance sont consignés dans un document confidentiel et peuvent être consultés par le RPD et le responsable délégué du traitement.

Des caméras de RAPI sont également déployées et servent de moyens pour faciliter l'accès du personnel et de leurs véhicules aux parcs de stationnement situés dans les locaux de l'OEB.

Les zones soumises à des attentes plus élevées en matière de protection de la vie privée, telles que les bureaux, les espaces de loisirs, les cantines, les bars, les cafétérias, les toilettes, les douches et les vestiaires, ne sont pas surveillées.

Une analyse d'impact relative à la protection des données est effectuée dans tous les cas où l'opération de traitement est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes concernées.

(d) Exactitude

Le responsable délégué du traitement veille à ce que les données personnelles soient exactes et actualisées, en s'assurant que toutes les données inexactes soient effacées ou corrigées sans délai, compte tenu des finalités pour lesquelles elles sont traitées.

Pour appliquer ce principe, le responsable délégué du traitement met en place les procédures opérationnelles standard (POS) nécessaires, qui peuvent être consultées par le RPD. Les POS définissent les mesures prises pour garantir que les données personnelles traitées ou stockées dans le SVS sont régulièrement vérifiées, en veillant à ce que les données collectées soient actualisées et exactes. Les POS définissent également la procédure suivie pour corriger les données obsolètes ou inexactes chaque fois que de telles données sont découvertes par le responsable délégué du traitement ou déclarées par la personne concernée (article 19 RRPD : droit de rectification ; article 20 RRPD : droit d'effacement).

Le SVS est connecté au serveur de synchronisation de l'OEB, qui synchronise les journaux système des contrôles d'accès et de la gestion de la sécurité, ce qui garantit que tous les événements enregistrés par l'un ou l'autre sont correctement répertoriés.

(e) Limitation du stockage

Les données personnelles sont supprimées dès qu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées.

Vu la base juridique et les finalités du traitement des données personnelles à l'aide du SVS, la durée de conservation maximale des images captées est fixée à sept jours[1], après quoi les images sont automatiquement effacées. Cette durée de conservation peut être prolongée pour les sauvegardes d'images liées à des incidents identifiés pour lesquels les séquences constituent des preuves dans le cadre d'enquêtes, de recours, de litiges ou de réclamations. Elle peut être prolongée jusqu'à ce que les enquêtes, recours, litiges ou réclamations soient réglés.

(f) Intégrité et confidentialité

Le responsable délégué du traitement veille à ce que toutes les mesures techniques et organisationnelles appropriées soient en place pour maintenir la sécurité et la confidentialité des données personnelles, ce qui couvre également la protection contre la perte, l'endommagement, la destruction, les dégâts ou la diffusion d'origine accidentelle. Les mesures de sécurité sont analysées et régulièrement revues et adaptées au cas par cas.

Conformément au point 6.9 des Conditions contractuelles générales et, le cas échéant, des conditions prévues dans les accords sur le traitement des données signés avec les sociétés, tous les fournisseurs qui traitent des données personnelles s'assurent qu'elles sont traitées conformément aux lois et règlements applicables, et en particulier conformément au RRPD. Le personnel interne est également tenu d'appliquer le RRPD.

Le responsable délégué du traitement est responsable de la mise en œuvre des mesures techniques et organisationnelles nécessaires qui garantissent l'intégrité et la confidentialité

[1] Les durées de conservation des autres catégories de données figurent dans le registre des activités de traitement du SVS.

des données personnelles traitées ou stockées dans le SVS. Ces mesures sont proportionnelles au risque de destruction, d'altération, d'accès non autorisé ou de divulgation que le SVS comporte pour les droits et libertés des personnes concernées.

Mesures de protection

Les données personnelles traitées ou stockées dans le SVS sont protégées de manière à permettre la séparation des fonctions et à limiter l'accès aux données personnelles en fonction des rôles et des fonctions.

Dans la mesure de ce qui est possible techniquement, le responsable délégué du traitement met en œuvre les contrôles applicables en vertu de la norme ISO 27001, en particulier ceux qui ont été établis pour les appareils mobiles et le télétravail, la sécurité des ressources humaines, la gestion des actifs, la gestion des médias, le contrôle d'accès, la cryptographie, les zones sécurisées et la sécurité des équipements.

Des contrôles internes réguliers (tests de vulnérabilité) sont effectués pour vérifier l'intégrité, la confidentialité et la disponibilité du système et de ses composants, ainsi que le niveau de conformité avec les contrôles mentionnés ci-dessus.

L'accès à l'application du SVS nécessite une authentification via des outils BIT (mot de passe/active directory) plus un mot de passe supplémentaire pour l'application[2].

Toutes les images enregistrées sont chiffrées. L'ensemble des données à caractère personnel est conservé dans des applications informatiques sécurisées conformément aux normes de sécurité de l'OEB. Ces normes de sécurité sont :

- authentification de l'utilisateur : tous les postes de travail et serveurs requièrent une ouverture de session, les dispositifs mobiles de l'OEB requièrent une ouverture de session au site de l'OEB, les comptes privilégiés requièrent une authentification supplémentaire et plus stricte ;
- contrôle d'accès (p. ex. contrôle de l'accès aux systèmes et au réseau en fonction du rôle, principes du "besoin de savoir" et du "moindre privilège") ; séparation des rôles d'administrateur et d'utilisateur, les utilisateurs ayant un minimum de privilèges et les rôles d'administrateur étant limités au minimum ;
- renforcement de la sécurité des systèmes, équipements et réseaux : 802.1x pour l'accès au réseau, chiffrement des dispositifs de point d'extrémité, installation d'antivirus sur tous les dispositifs ;
- protection physique : contrôles des accès effectués à l'OEB, contrôles supplémentaires des accès au centre de données, politiques relatives à la fermeture des bureaux ;
- contrôle des transmissions et entrées (p. ex. journaux d'audit, surveillance des systèmes et réseaux) : surveillance de la sécurité avec un logiciel spécialisé qui analyse les données générées par les machines pour détecter les menaces ;
- intervention en cas d'incident de sécurité : surveillance des incidents 24 heures sur 24 et 7 jours sur 7, expert en sécurité de garde.

[2] Mise en œuvre à La Haye, cette mesure sera appliquée aux autres sites de l'OEB dans un avenir proche.

Accès aux données à caractère personnel

Un nombre limité de personnes ayant besoin de savoir et régulièrement formées à la protection des données ont la permission d'accéder à des données personnelles ou aux systèmes dans lesquels celles-ci sont traitées ou stockées. La liste des personnes ayant un droit d'accès est contenue dans le document confidentiel "Liste des personnes ayant accès au SVS et de leurs droits d'accès".

L'accès de chaque personne est basé sur son rôle et ses responsabilités et est toujours limité, du point de vue de la durée et des finalités, au minimum requis pour accomplir ses tâches spécifiques (par exemple, sécurité, maintenance, administration de systèmes).

Le personnel de sécurité chargé de la protection des bâtiments de l'OEB a accès aux 60 dernières minutes des enregistrements. La finalité de cet accès est le traitement des alarmes et l'assistance en cas d'urgence pendant cette durée limitée.

La liste des personnes ayant accès à des données personnelles ou à des systèmes dans lesquels elles sont traitées ou stockées est régulièrement revue et mise à jour. Les procédures d'octroi, de modification et de révocation des accès peuvent être facilement consultées.

L'accès aux données personnelles stockées dans le système (par exemple pour évaluer un incident) nécessite l'approbation préalable du responsable délégué du traitement, qui peut consulter le RPD. Tous les détails concernant l'accès aux données personnelles sont consignés dans le document "Accès aux journaux de données personnelles".

Divulgation de données à caractère personnel

Les données personnelles traitées ou stockées dans le SVS ne sont utilisées qu'en interne par le département de l'OEB exploitant le VSS et le personnel de son prestataire de services de sécurité externe pour les aider dans l'exercice de leurs fonctions.

Les autres personnes ont le droit d'accéder à leurs données personnelles en adressant une demande en ce sens au responsable délégué du traitement, qui peut consulter le RPD pour obtenir des conseils.

En cas de comportement de conduite extrêmement dangereux, le responsable délégué du traitement peut fournir aux experts de la sécurité de l'OEB un accès à la vidéo afin qu'ils l'analysent et formulent des conseils, en consultant le RPD pour avis si nécessaire.

Dans le cas d'accidents ou d'incidents impliquant des déclarations de sinistre, le responsable délégué du traitement peut également donner accès aux extraits vidéo pertinents à la société traitant le sinistre, à condition que toutes les dispositions pertinentes du RRPD pour cette divulgation soient respectées.

Le responsable délégué du traitement tient un registre précis qui documente la divulgation, y compris son fondement juridique, la date et l'heure, le type de données personnelles divulguées et les destinataires.

Article 4 – Droits individuels

Droit d'être informé

(1) Les personnes ont le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel les concernant sont ou ne sont pas traitées. Les personnes concernées recevront des informations conformément à l'article 16 du RRPD. Des informations sur la présence du SVS seront mises à la disposition du public. Ces informations seront fournies selon une approche par niveaux successifs, qui est décrite ci-après.

(2) Le premier niveau d'information consiste en une signalisation. Les panneaux, d'une taille adaptée à leur emplacement, seront clairement visibles et lisibles. Ils indiqueront l'identité du responsable délégué du traitement, la finalité des opérations de traitement et les coordonnées de contact. Ils renverront également à des informations supplémentaires pertinentes, par exemple aux droits des personnes concernées. Ce renvoi pourra prendre la forme d'un lien ou d'un code QR vers un site où les personnes concernées pourront facilement trouver les informations.

(3) Le deuxième niveau est constitué par la présente politique, qui est accessible via les liens figurant sur les panneaux d'avertissement et dont un exemplaire papier peut être facilement consulté à l'accueil des bâtiments de l'OEB.

(4) Il n'est pas nécessaire de rendre publiques les positions des caméras, dès lors qu'il est facile pour les personnes concernées de s'apercevoir qu'elles pénètrent dans des zones surveillées.

Autres droits des personnes concernées

(1) Les personnes enregistrées par le SVS disposent des droits suivants : droit d'accès aux séquences, droit de rectification, droit d'opposition, droit d'effacement et droit de limitation du traitement.

(2) Les personnes concernées peuvent exercer l'un des droits susmentionnés en adressant une demande écrite au responsable délégué du traitement, qui répondra dans un délai d'un mois à compter de la date de réception de la demande.

(3) Le responsable délégué du traitement traitera les demandes d'accès aux données personnelles et les demandes visant à ce qu'elles soient fournies, effacées, corrigées, rectifiées ou complétées dans les plus brefs délais et au plus tard un mois après la réception de la demande.

(4) Le responsable délégué du traitement peut refuser de fournir l'information s'il peut être prouvé que la demande est manifestement infondée ou excessive.

Article 5 – Formation

(1) Le RPD promeut des programmes réguliers de formation à la protection des données et sensibilise le personnel de l'OEB impliqué dans les opérations de traitement. Les gestionnaires

de contrat des fournisseurs intervenant dans les opérations de traitement s'assurent que le personnel du fournisseur est adéquatement formé à se conformer à la présente politique.

(2) La formation, qui est obligatoire pour tout le personnel ayant accès à des données personnelles en direct ou enregistrées, couvrira au minimum les risques que les opérations de traitement comportent pour les données à caractère personnel, et insistera sur les précautions à prendre lorsque des données à caractère personnel de catégories particulières sont traitées. Les points suivants seront abordés :

- Politique de l'OEB en matière d'enregistrement et de conservation des informations ;
- Comment gérer les informations en toute sécurité ;
- Que faire lorsqu'une demande de renseignements est reçue, par exemple de la part de la police ;
- Comment reconnaître une demande d'une personne concernée et que faire lorsqu'une telle demande est reçue ;

Article 6 – Documents que le responsable délégué du traitement doit tenir à jour (confidentiel)

- Carte montrant l'emplacement de toutes les caméras de vidéosurveillance
- Test de vulnérabilité, y compris résultats, liste d'actions et état d'achèvement
- Analyse d'impact relative à la protection des données
- Journal des formations à la protection des données
- Accès aux journaux de données personnelles
- Liste des personnes ayant accès au SVS et de leurs droits d'accès
- Procédure opérationnelle standard (POS) pour l'octroi, la modification et la révocation des accès physiques et logiciels
- POS de vérification de l'exactitude des données personnelles traitées ou stockées
- Contrat avec les prestataires de services de sécurité
- Modèle de sécurité de l'OEB, y compris zones de sécurité

Article 7 – Coordonnées

Les personnes peuvent adresser leurs questions au responsable délégué du traitement de l'OEB à l'adresse e-mail suivante : dpl.pd44@epo.org.

Vous pouvez consulter le RPD à l'adresse e-mail suivante : dpo@epo.org.

Annexes

- Règlement relatif à la protection des données
- Circulaire n° 380
- Circulaire n° 381

Munich, le 16.12.2022.

Le Président de l'Office européen des brevets

António Campinos