Groupe Banque européenne d'investissement

Politique de vidéosurveillance

Groupe
Banque européenne
d'investissement

TABLE DES MATIERES

1. Objet et champ d'application de la politique de vidéosurveillance

Ce document présente la politique de gestion des systèmes de vidéosurveillance, en fonction des besoins et contraintes de la Banque en matière de sécurité, dans le respect des textes de références à savoir i) le règlement n°45/2001 du 18 décembre 2000 (« **le règlement** ») ii) les lignes directrices publiées par le Contrôleur Européen de la Protection des Données (« **le CEPD** ») en date du 17 mars 2010, minimisant l'impact de la vidéosurveillance sur la vie privée et les autres droits fondamentaux.

2. Respect de la vie privée, protection des données et conformité avec la réglementation.

2.1. État de conformité.

L'unité Sécurité et Services au sein de la Division Facilities Management i) définit les systèmes de vidéosurveillance en adéquation avec les besoins de la Banque en matière de sécurité ii) assure la conformité des équipements et du système en général par rapport aux recommandations du CEPD iii) pilote et gère la coordination entre les différentes parties prenantes.

2.2. Audit

Lors de toute modification notoire du système, la Banque effectue un audit et une analyse d'impact de ces modifications. Dans tous les cas, le Délégué à la Protection des Données (« DPD ») de la Banque ainsi que la Représentation du Personnel au travers du Comité Paritaire pour la Prévention et Protection au Travail (« CPPPT ») sont impliqués à la source dans ces processus.

2.3. Notification de l'état de conformité au CEPD.

Compte tenu du déploiement limité du système, la Banque n'a pas jugé nécessaire de réaliser une analyse d'impact ou de soumettre une notification de contrôle préalable au CEPD des installations existantes.

Lors de l'adoption de la présente politique de vidéosurveillance, nous avons par ailleurs notifié notre état de conformité au CEPD en lui adressant un exemplaire de notre politique de vidéosurveillance et du rapport d'audit.

2.4. Décision d'installer la vidéosurveillance au sein de la BEI.

La vidéosurveillance a été mise en place dans le cadre de la mise en sureté globale du complexe immobilier du Siège de la BEI.

2.5. Transparence.

La politique de vidéosurveillance existe en deux versions, l'une à diffusion restreinte, l'autre publique (la présente version). La version publique est consultable sur notre intranet ainsi que sur nos sites Web aux adresses suivantes : http://www.eib.org/ et http://www.eif.org/ .
La présente version publique de la politique de vidéosurveillance est une synthèse de la politique générale de la Banque en la matière. Pour des raisons de sécurité, certaines informations confidentielles ne sont pas reprises dans le présent document mais peuvent être consultées sur demande.

Par ailleurs, des affichages au niveau des réceptions et dans les bâtiments sont en place afin de signaler aux usagers ainsi qu'aux visiteurs que les sites de la Banque sont sous vidéosurveillance.

2.6. Examens périodiques.

Un examen des systèmes de vidéosurveillance est réalisé par l'Unité Sécurité et Service tous les deux ans, le prochain devant intervenir pour Septembre 2013 au plus tard. Lors de ces examens périodiques, sont réévalués:

- l'utilité du système de vidéosurveillance ;
- son adéquation avec les finalités pour lesquelles il a été conçu ;
- l'existence éventuelle d'alternatives appropriées.

Les examens périodiques servent à vérifier notamment si la politique de vidéosurveillance est toujours conforme au règlement et aux lignes directrices. Ces audit sont effectués par des sociétés spécialisées externes.

2.7. Solutions techniques favorisant le respect de la vie privée.

Les principales solutions techniques mises en œuvre favorisant le respect de la vie privée, s'orientent autour de 2 axes principaux, à savoir :

- la position et les angles de prises de vues des caméras sont établis de manière à ne filmer que les parties privatives (site BEI). De plus, les zones des bâtiments pour lesquels les attentes en matière de respect de la vie privée sont élevées (p.ex. : les bureaux, les espaces de détente, les toilettes, les vestiaires,…) ne sont pas surveillés par des caméras de vidéosurveillance
- L'accès aux données enregistrées n'est autorisé que par mot de passe et pour la seule personne responsable du traitement des données, à savoir le responsable de l'Unité Sécurité et Services de la Banque. Il peut déléguer ces droits à une personne désignée.

3. Espaces placés sous vidéosurveillance

Pour la protection des biens et pour assurer la sécurité du personnel et des visiteurs, les espaces suivants sont sous vidéosurveillance :

- Les espaces regroupant des informations sensibles, des biens de grande valeur ou autres actifs qu'ils contiennent et qui nécessitent une protection renforcée pour une raison bien spécifique ;
- les entrées et les sorties des bâtiments (y compris les issues de secours, ainsi que les murs et les clôtures entourant les bâtiments ou le site) ;
- les entrées et les sorties de différentes zones d'un bâtiment soumises à des régimes différents en matière de droits d'accès et séparées par des portes de sûreté ou par d'autres mécanismes de contrôle des accès.

4. Type d'informations à caractère personnel collecté et finalité

4.1. Brève description et caractéristiques techniques du système.

Chaque bâtiment de la Banque est équipé d'un système de vidéosurveillance. Chaque système est conçu selon le même principe. Seules les quantités de matériel (caméras, enregistreurs) changent selon la taille du site et les besoins en matière de sécurité.
Etant donné que chaque bâtiment est équipé de son propre système, les images provenant des caméras qui y sont installées sont gérées et traitées localement.

Le système se compose de plusieurs enregistreurs numériques équipés chacun d'un disque dur où sont stockées les images et d'un dispositif de détection de mouvement. Il enregistre tous les mouvements détectés par les caméras dans les zones placées sous surveillance, ainsi que la mention de la date, de l'heure et du lieu d'enregistrement. Toutes les caméras fonctionnent 24h/24, sept jours sur sept.

Certaines zones extérieures sensibles, et non accessibles au public, sont surveillées par des caméras équipées de phares infrarouge pour la surveillance nocturne.

Aucun système de vidéosurveillance de haute technologie ou « intelligent », d'enregistrements sonores, de vidéosurveillance parlante ou de surveillance dissimulée n'est en place à la Banque. Des dérogations, pour des raisons exceptionnelles et limitées dans le temps font obligatoirement l'objet d'une notification préalable au CEPD et/ou DPD de la Banque.

La liste des caméras et des enregistreurs par site est jointe en annexe de la politique détaillée et peut être consultée sur demande (Cf. §10 et 11) .

4.2. Objet de la surveillance.

La Banque utilise son système de vidéosurveillance à des fins de sécurité et de contrôle d'accès exclusivement. Le système de vidéosurveillance facilite le contrôle des accès aux locaux et contribue à assurer la protection des infrastructures, la sécurité du personnel et des visiteurs, ainsi que la protection des biens et des informations situées ou stockées dans les locaux. Il intervient en complément d'autres systèmes de sécurité physique tels que les systèmes de contrôle des accès et des intrusions physiques. Il fait partie des mesures adoptées pour renforcer les mesures plus générales appliquées dans le domaine de la sécurité et contribue à prévenir, à dissuader et, si nécessaire, à rechercher les accès physiques non autorisés, y compris à des locaux sécurisés ou placés sous protection, à des infrastructures informatiques, ou à des informations opérationnelles. De plus, la vidéosurveillance contribue à prévenir, à détecter et à enquêter sur les vols d'équipements ou de matériel appartenant à la Banque, à ses visiteurs ou à son personnel, ainsi que les atteintes à la sécurité des visiteurs ou du personnel travaillant dans les locaux (incendies ou agressions physiques, par exemple).

4.3. Limitation des finalités.

Le système n'est utilisé à nulles autres fins que celles exposées ci-dessus. Il n'est pas utilisé pas pour surveiller le travail des employés ou pour contrôler leur présence sur leur lieu de travail. Il n'est pas non plus utilisé à des fins d'enquête (autres que celles faisant suite à des incidents de sécurité physique tels que des vols ou des accès non autorisés). Les éventuels transferts d'images vers des organes d'enquête ne peuvent avoir lieu que dans des circonstances exceptionnelles, dans le cadre d'enquêtes disciplinaires ou judiciaires, conformément aux dispositions de la politique générale de vidéosurveillance.
L'utilisation et le traitement des données à des fins d'enquêtes font l'objet d'une validation préalable par le DPD et/ou le CEPD

4.4. Activités de surveillance ponctuelle.

En cas d'activité de vidéosurveillance ponctuelle, un registre des interventions est tenu à jour par l'Unité Sécurité et Services pour toute consultation de données.

4.5. Absence de collecte de catégories particulières de données.

Les systèmes de vidéosurveillance en place dans les bâtiments de la Banque n'ont pas pour objet de capter (en zoomant ou en orientant délibérément la caméra à cette fin, par exemple) ou, d'une manière générale, de traiter des images (en les indexant ou en établissant des profils) susceptibles de révéler des « catégories spéciales de données », à savoir : l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé ou à la vie sexuelle[1].

Aucune surveillance de zones propices à la révélation, par les images captées, de données relevant de ces catégories particulières n'est effectuée par les systèmes vidéosurveillance de la Banque.

[1] Voir l'article 10 du règlement.

5. Qui a accès aux données collectées et à qui sont-elles communiquées ?

5.1. Le personnel chargé de la sécurité interne et les agents de sécurité externes.

Les enregistrements de vidéosurveillance sont uniquement accessibles au responsable du traitement des données, à savoir le Chef d'unité Sécurité et Services. Les agents de sécurité ont également accès aux images filmées en direct pendant leurs heures de service mais uniquement en mode visualisation sans possibilité d'effectuer des recherches ou des relectures. Ces agents travaillent pour une entreprise de sécurité sous-traitante présente sur site.

5.2. Droits d'accès.

La politique générale de vidéosurveillance de la Banque mentionne de façon claire et précise qui a accès aux images filmées ou à l'architecture technique du système de vidéosurveillance ; dans quel but ces droits d'accès sont créés et en quoi ils consistent. Ce document précise notamment qui est autorisé à :

- visionner les images en temps réel ;
- visionner les images enregistrées ;
- copier ;
- télécharger ;
- effacer ;
- exporter les données
- effectuer la maintenance technique ..

5.3. Formation du personnel à la protection des données.

Tous les membres du personnel dotés de droits d'accès, y compris les agents de sécurité externes, ont reçu une formation à la protection des données**.** Les nouveaux membres du personnel de sécurité reçoivent systématiquement une formation à leur arrivée dans le service. (cf. point 8.2 de la politique générale).

5.4. Engagement de confidentialité du personnel de sécurité.

À la fin de leur formation, tous les membres du personnel de sécurité ont signé un engagement de confidentialité. Cet engagement fait partie intégrante du contrat de l'entreprise sous-traitante. Ces engagements sont inclus dans les conditions générales de la Banque jointes à tout contrat de sous-traitance ou de consultance.

5.5. Transfert et communication de données.

L'éventuel transfert ou communication de données ne peut se faire que par le responsable du traitement des données, à savoir le Chef d'unité Sécurité et Services, et avec information préalable du Délégué à la Protection des Données (DPD) de la Banque et/ou du Contrôleur Européen de la Protection des Données (CEPD). Tout acte de transfert et de communication de données à des destinataires extérieurs au service de Sécurité sont répertoriés et font l'objet d'une évaluation rigoureuse quant à leur nécessité et à la compatibilité de leurs finalités avec celles initialement poursuivies, à savoir la sécurité et le contrôle d'accès

Ces transferts sont consignés dans un registre tenu par l'Unité Sécurité et Service.
Le personnel de Direction et le Département des Ressources Humaines ne disposent d'aucun droit d'accès aux données.

6. Comment est assurée la protection des données collectées ?

Afin d'assurer la sécurité du système de vidéosurveillance, et notamment celle des données à caractère personnel, un certain nombre de dispositions ont été prises sur les plans technique et organisationnel. Ces dispositions sont détaillées dans la politique générale de vidéosurveillance de la Banque.

Quelques-unes des mesures mises en place sont :

- les serveurs sur lesquels les images sont stockées se trouvent dans des locaux sécurisés, protégés par des dispositifs de sécurité physique ; des dispositifs pare-feu protègent le périmètre de l'infrastructure informatique. Enfin, les principaux systèmes informatiques qui renferment les données bénéficient de mesures de protection renforcées ;
- les droits d'accès accordés aux utilisateurs leur permettent d'accéder uniquement aux ressources absolument indispensables à l'accomplissement de leurs tâches ;
- seul l'administrateur du système, spécialement désigné à cet effet par le responsable du traitement, est en mesure d'accorder, de modifier ou d'annuler les droits d'accès d'une personne. Tout octroi, modification ou annulation de droits d'accès est régi par les critères établis au sein de la politique générale de sécurité en matière de vidéosurveillance
- la politique générale de sécurité en matière de vidéosurveillance comporte une liste mise à jour de l'ensemble des personnes qui ont accès au système à tout moment et décrit en détail leurs droits d'accès.

7. Durée de conservation des données

Les images sont conservées pour une durée de 21 jours au maximum. Au-delà, les enregistrements sont systématiquement détruits. Si nécessaire, les images pouvant être utilisées à des fins d'enquête ou de preuve suite à un incident de sécurité peuvent être conservées plus longtemps. Leur conservation est rigoureusement consignée et la nécessité de leur conservation est régulièrement réexaminée.

8. Information du public

8.1. Approche multicouche.

Est mise en place à l'intention du public une information appropriée et exhaustive sur nos activités de vidéosurveillance. Cette information se fait selon une approche multicouche qui associe les deux mesures suivantes :

- l'installation sur place de panneaux d'information destinés à signaler au public la présence d'un dispositif de surveillance et à lui fournir des informations essentielles sur le traitement des données ;
- la publication de la présente politique de vidéosurveillance sur l'intranet ainsi que sur nos sites Web à l'intention des personnes qui souhaiteraient en savoir plus sur les activités de vidéosurveillance de notre institution.
- possibilité de consulter une version papier de la politique générale de vidéosurveillance sur demande auprès du service de sécurité. Un numéro de téléphone et un numéro de Téléfax sont à la disposition des personnes souhaitant obtenir des informations complémentaires.

Sont également installés des panneaux d'information à proximité des espaces surveillés, notamment près de l'entrée principale, des ascenseurs desservant les parkings et des l'entrées du parking visiteurs.

8.2. Notifications individuelles.

Outre ces mesures, les personnes identifiées grâce aux caméras (par exemple, par les agents de sécurité dans le cadre d'une enquête de sécurité) en sont également informées individuellement dès lors qu'une ou plusieurs des conditions suivantes s'appliquent :

- leur identité est mentionnée dans un fichier ;
- l'enregistrement vidéo est utilisé à leur encontre ;
- il est conservé au-delà de sa durée normale de conservation ;
- il est transféré à l'extérieur du service de sécurité ;
- l'identité de la personne concernée est communiquée à des destinataires extérieurs au service de sécurité.

La communication de ces notifications peut être temporairement retardée, par exemple lorsqu'un délai est nécessaire à la prévention, à la recherche, à la détection ou à la poursuite d'infractions pénales[2]. Une consultation systématique et immédiate du DPD (Délégué à la Protection des Données) est effectuée pour tous les cas de ce type afin de garantir le respect des droits de la personne concernée.

9. Accès du public aux données

Le public est en droit d'accéder aux données à caractère personnel le concernant qui se trouvent en possession de la Banque afin de les faire rectifier ou effacer.

Les modalités d'accès à ces données pour toute rectification, blocage ou d'effacement sont à coordonner avec :

- **le Chef d'Unité Sécurité et Services, Responsable du traitement des données**
  100 boulevard Konrad Adenauer
  L-2950 Luxembourg
  tel : 4379-1

Il peut également être contacté pour toute question relative au traitement de données à caractère personnel.

[2] D'autres exceptions énumérées à l'article 20 du règlement peuvent également s'appliquer dans des circonstances exceptionnelles.

10. Droit de recours

Toute personne a le droit de saisir le Contrôleur européen de la protection des données (edps@edps.europa.eu) si elle estime que les droits qui lui sont reconnus par le règlement (CE) n° 45/2001 ont été violés consécutivement au traitement par la Banque de données à caractère personnel la concernant. Avant d'engager une telle procédure, nous conseillons aux personnes souhaitant déposer un recours de contacter :

- **le Chef d'Unité Sécurité et Services, Responsable du traitement des données**
  100 boulevard Konrad Adenauer
  L-2950 Luxembourg
  tel : 4379-1

- **le Délégué à la Protection des Données (DPD) de la Banque**
  100 boulevard Konrad Adenauer
  L-2950 Luxembourg
  tel : 4379-1

Toute personne concernée peut obtenir, selon l'article 14 du règlement, un droit de rectifications de données dans le cas ou celles-ci la concernant seraient erronées en s'adressant au chef d'Unité Sécurité et Services. Après vérification des données, le chef d'Unité Sécurité et Services apportera les modifications adéquates et ce dans un délais de quinze jours après demande de rectifications.

Dans le cas d'une demande d'effacement, une consultation du DPD sera effectuée par le chef d'unité sécurité et Services. Dès réception de l'avis du DPD, ou du CEPD le cas échéant, confirmant la nécessité d'effacement des données, le chef d'Unité Sécurité et Services procèdera à leur effacement.

Groupe
Banque européenne
d'investissement

Contacts

Pour tout renseignement d'ordre général :

Banque européenne d'investissement

Banque européenne d'investissement
98-100, boulevard Konrad Adenauer
L-2950 Luxembourg
(+352) 43 79 - 1
(+352) 43 77 04
www.bei.org

EUROPEAN INVESTMENT FUND

EIF headquarters
96, boulevard Konrad Adenauer
L-2968 Luxembourg
(+352) 24 85 1
(+352) 24 85 81301
info@eif.org