COUR DES COMPTES EUROPÉENNE
Secrétariat général

Cour des comptes européenne

Sécurité de l'information

Politique en matière de vidéosurveillance

ÉTAT D'AVANCEMENT DU DOCUMENT ET RELEVÉ DES RÉVISIONS

État d'avancement du document

Politique n°	
Classification	Interne à la Cour
État	Approuvé
Personne de contact	Dimitrios Vavatsis

Réviseur(s)	**Réviseur(s)**	**Approbateur(s)**
J. Van Damme		N. Usher

Relevé des révisions

Révision	Date	Qui?	Description	Parties concernées
Projet	20101112	D. Vavatsis	Initial	Toutes
Révision	20110802	J. Van Damme	Examen	Toutes
Doc. approuvé	20111026	N. Usher	Approuvé	Toutes

TABLE DES MATIÈRES

ÉTAT D'AVANCEMENT DU DOCUMENT ET RELEVÉ DES RÉVISIONS 2
État d'avancement du document 2
Relevé des révisions 2
1. INTRODUCTION 4
2. OBJECTIFS DU DOCUMENT 4
3. CHAMP D'APPLICATION 4
4. GARANTIR UNE UTILISATION EFFICACE ET CIBLÉE DE LA VIDÉOSURVEILLANCE 4
4.1. Révision du système existant 4
4.2. Audit interne 4
4.3. Notification du statut de conformité au CEPD 4
4.4. Contacts avec l'autorité de protection des données compétente dans l'État membre 5
4.5. Décision du Secrétaire général et consultation 5
4.6. Transparence 5
4.7. Contrôles périodiques 5
4.8. Solutions technologiques respectueuses de la vie privée 6
5. ENDROITS SOUS SURVEILLANCE 6
6. COLLECTE DES INFORMATIONS PERSONNELLES ET FINALITÉ 6
6.1. Description sommaire et spécifications techniques détaillées du système 6
6.2. Objectif de la surveillance 7
6.3. Restriction de la finalité 7
6.4. Pas de surveillance *ad hoc* prévue 7
6.5. Webcams 7
6.6. Collecte de catégories spéciales de données 7
7. ACCÈS AUX INFORMATIONS ET DIVULGATION DE CELLES-CI 8
7.1. Personnel de sécurité interne 8
7.2. Formation à la protection des données 8
7.3. Accords de confidentialité 8
7.4. Transferts et divulgations 8
7.5. Comment les informations sont-elles protégées et sauvegardées? 9
8. PENDANT COMBIEN DE TEMPS LES INFORMATIONS SONT-ELLES CONSERVÉES? 9
9. INFORMATIONS COMMUNIQUÉES AU PUBLIC 9
9.1. Approche à plusieurs niveaux 9
9.2. Notification individuelle spécifique 10
10. VÉRIFICATION, CORRECTION ET SUPPRESSION D'INFORMATIONS 10
11. DROIT DE RECOURS 11
12. RÉFÉRENCES 11

1. INTRODUCTION

La Cour des comptes européenne (ci-après «la CdCE») utilise un système de vidéosurveillance afin d'assurer la sécurité de ses bâtiments, de ses biens, de son personnel et de ses visiteurs. La présente politique de vidéosurveillance et ses annexes décrivent le système de vidéosurveillance de la CdCE et les précautions qu'elle prend pour protéger les données à caractère personnel, le droit à la vie privée et les autres droits fondamentaux et intérêts légitimes des personnes filmées par les caméras du système.

2. OBJECTIFS DU DOCUMENT

Garantir un traitement des images de vidéosurveillance qui soit conforme aux lignes directrices et au règlement (CE) n° 45/2001 relatif à la protection des données à caractère personnel par les institutions et organes communautaires.

3. CHAMP D'APPLICATION

L'ensemble des systèmes de vidéosurveillance installés dans les bâtiments de la CdCE et gérés par elle. Loués par la Cour, les bâtiments K9 et K7, qui sont gérés par le propriétaire pour le premier et par la Cour de justice pour le second, ne relèvent pas du champ d'application du présent document.

4. GARANTIE D'UNE UTILISATION EFFICACE ET CIBLÉE DE LA VIDÉOSURVEILLANCE

4.1. Révision du système existant

La CdCE utilisait déjà un système de vidéosurveillance avant que le Contrôleur européen de la protection des données (CEPD) ne publie les lignes directrices en matière de vidéosurveillance (ci-après «les lignes directrices») le 17 mars 2010. Depuis lors, la CdCE a cependant revu ses procédures conformément aux recommandations formulées au chapitre 15 des lignes directrices.

4.2. Audit interne

Le système a fait l'objet d'un audit interne et le rapport correspondant est joint en tant qu'annexe 1.

4.3. Notification du statut de conformité au CEPD

Une analyse d'impact sur la vie privée a été réalisée (voir annexe 2).

Une notification de contrôle préalable a été soumise au CEPD (voir chapitre 4.3 des lignes directrices) le 26 octobre 2011 (annexe 3) et l'avis du CEPD sur cette notification est joint en tant qu'annexe 4 (en attente).

Parallèlement à l'adoption de la présente politique en matière de vidéosurveillance, la CdCE a également communiqué son statut de conformité au CEPD en lui adressant un exemplaire de cette politique et du rapport d'audit initial.

4.4. Contacts avec l'autorité de protection des données compétente dans l'État membre

L'autorité de protection des données compétente au Luxembourg, la CNPD, a été informée. Par ailleurs, l'avis affiché sur place et la présente politique de vidéosurveillance sont également disponibles en anglais et en allemand.

4.5. Décision du Secrétaire général et consultation

La décision d'utiliser le système de vidéosurveillance actuel et d'adopter les mesures de protection décrites dans cette politique de vidéosurveillance a été prise par le Secrétaire général après consultation:

- du directeur Finances et soutien, responsable de la sécurité physique,
- du délégué à la protection des données de la CdCE,
- du comité du personnel.

Durant ce processus de prise de décision, la CdCE a démontré et documenté la nécessité de recourir à un système de vidéosurveillance tel que celui proposé par cette politique, a envisagé d'autres solutions et conclu que le maintien du système de vidéosurveillance actuel, après l'adoption des garanties en matière de protection des données proposées dans le présent document, était à la fois nécessaire et adapté au regard des objectifs décrits au point 1 (voir chapitre 5 des lignes directrices), et a réagi aux préoccupations exprimées par le délégué à la protection des données et par le comité du personnel (voir chapitre 4 des lignes directrices).

4.6. Transparence

Il existe deux versions de la politique de vidéosurveillance: une version confidentielle à usage restreint et la présente version, publiée sur les sites internet et intranet de la CdCE à l'adresse www.eca.europa.eu/CCTV. La version publique contient parfois des informations sommaires concernant certains thèmes ou annexes. Le cas échéant, cela est toujours indiqué clairement. La version publique omet certaines informations uniquement dans les cas où la confidentialité est absolument nécessaire (par exemple pour des raisons de sécurité, pour garantir la confidentialité de certaines informations commercialement sensibles ou pour protéger la vie privée des personnes).

4.7. Contrôles périodiques

L'unité chargée de la sécurité procédera tous les deux ans à un contrôle en matière de protection des données. Le premier de ces contrôles aura lieu au plus tard le 31 mai 2013. Ils permettront de vérifier:

- si l'utilisation du système de vidéosurveillance reste nécessaire;
- si le système répond encore à son objectif initial, et s'il n'existe toujours pas de solutions de remplacement appropriées.

Les contrôles périodiques couvriront également toutes les questions abordées dans le premier rapport. Ils permettront notamment de vérifier si la politique de vidéosurveillance reste conforme au règlement et aux lignes directrices (audit

d'adéquation) et si cette politique est respectée en pratique (audit de conformité). Des copies des rapports de contrôle périodiques figureront également à l'annexe 1 de la présente politique de vidéosurveillance.

4.8. Solutions technologiques respectueuses de la vie privée

Les solutions suivantes, respectueuses de la vie privée, ont été déployées (voir chapitre 3.4 des lignes directrices):

- caméras basse résolution,
- technologie image par image.

5. ENDROITS SOUS SURVEILLANCE

Le système de vidéosurveillance se compose de 28 caméras. Un plan indiquant l'emplacement de celles-ci figure à l'annexe 5 (pour raisons de sécurité, cette annexe n'a pas été jointe).

Sur les 16 caméras installées au K1, 13 sont situées aux entrées et sorties du bâtiment, y compris l'entrée principale, les issues de secours et l'accès au garage. Les trois dernières sont installées dans le garage.

Le bâtiment K2 est équipé de huit caméras, dont cinq sont situées aux trois entrées et sorties protégées par un système de contrôle de l'accès, ainsi qu'à l'entrée du garage. Il y a également des caméras à l'entrée de la salle informatique, à l'intérieur de celle-ci et dans la salle de fitness.

Le K8 est équipé de quatre caméras: une à l'entrée principale, une à chacune des deux issues de secours et une à l'entrée du garage.

Il n'y a pas d'autre caméra ailleurs, que ce soit à l'intérieur ou à l'extérieur des bâtiments. Sauf dans la salle de fitness[1], aucune surveillance n'est exercée dans les endroits où les personnes peuvent s'attendre à un respect accru de leur vie privée, par exemple les bureaux individuels, les espaces de détente, les locaux sanitaires, etc. (voir chapitre 6.8 des lignes directrices). L'emplacement des caméras a été choisi avec soin de façon à limiter le plus possible la surveillance de zones ne présentant aucun intérêt au regard de l'objectif fixé (voir chapitre 6.1 des lignes directrices).

Il n'y a pas de surveillance à l'extérieur des bâtiments de la CdCE, sur le territoire du Luxembourg, comme cela est recommandé au chapitre 6.5 des lignes directrices.

6. COLLECTE DES INFORMATIONS PERSONNELLES ET FINALITÉ

6.1. Description sommaire et spécifications techniques détaillées du système

Le système de vidéosurveillance est un système statique traditionnel. Il effectue un enregistrement numérique image par image. Il enregistre les images prises par les caméras dans chaque zone surveillée ainsi que l'heure, la date et l'endroit. Toutes

[1] Une caméra a été installée dans la salle de fitness pour le cas où un utilisateur isolé serait victime d'un accident ou d'un malaise.

les caméras fonctionnent 24 heures sur 24, 7 jours sur 7. La qualité des images permet parfois d'identifier les personnes se trouvant dans le champ des caméras (voir chapitre 6.4 des lignes directrices). Celles-ci sont toutes fixes (pas de caméras à balayage horizontal, vertical et zoom) et ne peuvent donc pas être utilisées pour zoomer sur une cible ni pour suivre des personnes. Il n'est pas fait usage d'équipements de vidéosurveillance de haute technologie ou de vidéosurveillance intelligente (voir chapitre 6.9 des lignes directrices), le système n'est pas interconnecté avec d'autres systèmes (chapitre 6.10), et il n'y a ni surveillance dissimulée (chapitre 6.11), ni enregistrements sonores ou «caméras de surveillance parlantes» (chapitre 6.12).

6.2. Finalité de la surveillance

La CdCE utilise son système de vidéosurveillance exclusivement à des fins de sécurité et de contrôle des accès. Le système de vidéosurveillance facilite le contrôle des accès aux bâtiments de la CdCE et contribue à garantir la sécurité de ses bâtiments, de son personnel et de ses visiteurs, ainsi que l'intégrité des biens et des informations présents dans les locaux. Il s'ajoute au système de contrôle des accès. Il fait partie des mesures prises dans le cadre des politiques de sécurité plus générales de la CdCE et contribue à la prévention, à la dissuasion, et si nécessaire aux enquêtes relatives aux accès physiques non autorisés, y compris les accès non autorisés aux locaux sécurisés et aux pièces protégées, aux infrastructures informatiques ou aux informations opérationnelles. La vidéosurveillance contribue également à empêcher, détecter et élucider les vols de matériel ou de biens appartenant à la CdCE, à ses visiteurs ou à son personnel et à contrer les menaces pour la sécurité des visiteurs et du personnel travaillant dans ses locaux (par exemple incendie ou agression physique).

6.3. Restriction de la finalité

Le système n'est utilisé à aucune autre fin, comme, par exemple, le contrôle du travail ou de la présence des agents. Le système n'est pas non plus utilisé à des fins d'enquête (hormis pour enquêter sur les incidents de sécurité physique, tels que les vols et les accès non autorisés). Les images peuvent être communiquées aux organes d'investigation dans des circonstances exceptionnelles uniquement, en rapport avec une enquête criminelle ou disciplinaire formelle, comme celles décrites au point 7.4 (voir chapitres 5.7, 5.8 et 10.3 des lignes directrices).

6.4. Pas de surveillance *ad hoc* prévue

La CdCE n'envisage à ce stade aucune opération de surveillance *ad hoc* nécessitant une planification préalable (voir chapitre 3.5 des lignes directrices).

6.5. Webcams

Aucune webcam n'est installée à des fins de vidéosurveillance (voir chapitre 5.10 des lignes directrices).

6.6. Collecte de catégories spéciales de données

Aucune donnée relevant de catégories spéciales n'est collectée (voir chapitre 6.7 des lignes directrices).

7. ACCÈS AUX DONNÉES ET DIVULGATION DE CELLES-CI

7.1. Personnel de sécurité interne

Seul le personnel de sécurité interne a accès aux séquences enregistrées. Les images en direct sont également accessibles aux agents de sécurité en service. Ceux-ci n'ont accès qu'aux images en temps réel, l'administration du système étant assurée par les deux membres du personnel responsables de la sécurité physique, habilités à octroyer et à retirer les droits d'accès ainsi qu'à visionner les séquences enregistrées, à les copier, les télécharger et les supprimer.

7.2. Formation à la protection des données

Tous les membres du personnel possédant un droit d'accès ont reçu une formation de base à la protection des données. Chaque nouveau membre du personnel reçoit une formation, et des ateliers consacrés au respect des règles de protection des données sont organisés au moins une fois tous les deux ans à l'intention de tous les membres du personnel possédant un droit d'accès (voir chapitre 8.2 des lignes directrices).

7.3. Accords de confidentialité

Au terme de la formation, tous les membres du personnel concernés signent également un accord de confidentialité.

7.4. Transferts et divulgations

Tous les transferts et toutes les divulgations en dehors de l'unité de sécurité doivent être demandés formellement par écrit et documentés. Leur nécessité et la compatibilité de leur objectif avec la finalité première du système, à savoir la sécurité et le contrôle des accès, font l'objet d'une évaluation rigoureuse (voir chapitre 10 des lignes directrices). Un registre des séquences conservées et des transferts est joint en annexe 6 (vide) (voir chapitres 10.5 et 7.2 des lignes directrices). Le délégué à la protection des données est systématiquement consulté. Aucun accès n'est donné au personnel d'encadrement ou à la direction des ressources humaines.

Un accès peut être accordé à la police locale si cela s'avère nécessaire pour pouvoir enquêter sur des délits ou engager des poursuites. Dans des circonstances exceptionnelles, un accès peut également être accordé à l'Office européen de lutte antifraude (OLAF) dans le cadre d'une enquête menée par l'OLAF lui-même, à l'Office d'investigation et de discipline (IDOC) de la Commission dans le cadre d'une enquête disciplinaire, conformément aux règles définies à l'annexe IX du statut du personnel applicable aux fonctionnaires des Communautés européennes, ou aux organes chargés de mener une enquête interne ou une procédure disciplinaire au sein de l'institution. Ces transferts sont acceptables s'il y a des raisons de penser qu'ils peuvent faciliter l'enquête ou les poursuites relatives à une infraction disciplinaire suffisamment grave ou à un délit pénal. Les demandes en vue d'une exploration des données (*data mining*) sont systématiquement rejetées. Au cours des cinq dernières années, pour lesquelles la liste des transferts a été conservée, aucun transfert n'a été réalisé pour l'une des raisons énumérées ci-dessus.

7.5. Comment les informations sont-elles protégées et sauvegardées?

Un certain nombre de mesures techniques et organisationnelles ont été prises afin de garantir la sécurité du système de vidéosurveillance, y compris les données personnelles.

La politique de sécurité de la CdCE en matière de vidéosurveillance a été élaborée conformément au chapitre 9 des lignes directrices du CEPD en matière de vidéosurveillance.

Les mesures suivantes, entre autres, ont été prises:

- les ordinateurs servant à stocker les images enregistrées sont hébergés dans des locaux sécurisés, protégés par un contrôle électronique ou physique des accès; réseau spécial dissocié du réseau LAN de la CdCE, pas de connexion possible aux ordinateurs par port USB et absence de courrier électronique ou de toute autre connexion externe;

- tous les membres du personnel signent des accords de confidentialité et de non-divulgation;

- les utilisateurs ont accès uniquement aux informations qui leur sont strictement nécessaires pour s'acquitter de leurs fonctions.

Le responsable de la sécurité physique détient en permanence une liste à jour de toutes les personnes ayant accès au système, avec une description détaillée de la portée de leurs droits d'accès.

8. PÉRIODE DE CONSERVATION DES INFORMATIONS

Les images sont conservées pendant 16 jours au maximum (7 jours au bâtiment K8). Toutes les images sont ensuite physiquement écrasées par les nouvelles images enregistrées. Certaines images peuvent être gardées plus longtemps si leur conservation est nécessaire dans le cadre d'une enquête ou pour servir de preuve après un incident de sécurité. Cette conservation est rigoureusement documentée et sa nécessité est réévaluée régulièrement. Toute conservation d'images doit être notifiée au délégué à la protection des données, qui détient le registre de conservation et des transferts (voir chapitre 7 des lignes directrices).

Le système est également contrôlé en direct 24 heures sur 24 par l'agent de sécurité en service à la réception du bâtiment K1.

9. INFORMATIONS COMMUNIQUÉES AU PUBLIC

9.1. Approche à plusieurs niveaux

Les informations relatives à la vidéosurveillance sont communiquées au public de façon complète et effective (voir chapitre 11 des lignes directrices). À cette fin, une approche à plusieurs niveaux, associant les trois méthodes suivantes, a été adoptée:

- des avis affichés sur place permettant d'informer le public qu'une vidéosurveillance est en cours et de lui fournir les informations essentielles relatives au traitement des images. La présente politique de vidéosurveillance est publiée sur les sites intranet et internet de la CdCE;

- des exemplaires imprimés de cette politique de vidéosurveillance sont également disponibles sur demande à la réception du bâtiment et auprès de l'unité de sécurité. Un numéro de téléphone et une adresse électronique sont fournis pour ceux qui souhaitent obtenir de plus amples informations.

- des avis sont affichés à proximité des zones sous surveillance. Un avis est affiché à l'entrée du site, aux accès principaux et à l'entrée des salles sécurisées.

L'avis de protection des données affiché sur place par la CdCE est joint en tant qu'annexe 7.

9.2. Notification individuelle spécifique

Les personnes identifiées sur caméra (par exemple, par le personnel de sécurité dans le cadre d'une enquête de sécurité) doivent par ailleurs en être informées à titre individuel si au moins l'une des conditions suivantes est remplie:

- leur identité a été notée dans un dossier/un enregistrement;

- l'enregistrement vidéo est utilisé à l'encontre de la personne;

- l'enregistrement est conservé au-delà de la période de conservation normale;

- l'enregistrement est transféré en dehors de l'unité de sécurité;

- l'identité de la personne est communiquée à une personne extérieure à l'unité de sécurité.

Cette notification peut parfois être retardée temporairement, par exemple si un délai est nécessaire pour l'enquête ou pour la prévention, la détection ou la poursuite de délits. Le cas échéant, le délégué à la protection des données est systématiquement consulté afin de garantir le respect des droits de la personne concernée.

10. VÉRIFICATION, CORRECTION ET SUPPRESSION D'INFORMATIONS

Les membres du public ont le droit d'accéder aux données personnelles les concernant détenues par la CdCE, ainsi que de faire corriger et compléter ces données. Toute demande d'accès à des données à caractère personnel, ou de rectification, blocage et/ou suppression de celles-ci doit être adressée au responsable de la sécurité physique (ECA-Security@eca.europa.eu, tél. +352 4398-45400). Le délégué à la protection des données (ECA-Data-Protection@eca.europa.eu, tél. +352 4398-47777) peut également être contacté pour toute autre question relative au traitement de données à caractère personnel.

Dans la mesure du possible, le responsable de la sécurité apporte une réponse concrète aux demandes dans un délai de 15 jours calendrier. Si cela n'est pas possible, le demandeur est informé des étapes suivantes et de la raison du retard dans un délai de 15 jours. Même dans les cas les plus complexes, l'accès doit être accordé ou une réponse définitive et motivée rejetant la requête doit être fournie dans un délai maximal de trois mois. Le responsable de la sécurité fait tout ce qui est en son pouvoir pour réagir plus rapidement, surtout si le demandeur démontre l'urgence de sa requête.

En cas de demande spécifique, il est possible d'organiser un visionnage des images ou de fournir au demandeur une copie des images enregistrées, sur DVD ou sur un autre support. La personne qui introduit une demande de cette nature doit s'identifier formellement (par exemple en présentant sa carte d'identité avant le visionnage) et, dans la mesure du possible, préciser la date, l'heure, l'endroit et les circonstances dans lesquelles elle a été filmée. Elle doit également fournir une photographie récente permettant au personnel de sécurité de l'identifier sur les images en cours de visionnage.

À l'heure actuelle, la CdCE ne demande pas de contribution financière aux personnes souhaitant visionner les images sur lesquelles elles apparaissent ou en recevoir une copie. Elle se réserve cependant le droit de réclamer un montant raisonnable si le nombre de demandes d'accès devait augmenter.

Une demande d'accès peut être rejetée dans des cas précis soumis à une exemption au titre de l'article 20, paragraphe 1, du règlement (CE) n° 45/2001. Par exemple, au terme d'une évaluation au cas par cas, la CdCE peut arriver à la conclusion qu'un refus s'impose pour ne pas nuire à une enquête en cours concernant un délit. Une restriction peut également être nécessaire pour protéger les droits et les libertés d'autres personnes, par exemple lorsqu'elles sont également visibles sur les images et qu'il n'est pas possible d'obtenir leur consentement pour la divulgation de leurs données personnelles ou de modifier les images pour compenser l'absence de consentement.

11. DROIT DE RECOURS

Toute personne a le droit de saisir le contrôleur européen de la protection des données (edps@edps.europa.eu) si elle considère que ses droits garantis par le règlement (CE) n° 45/2001 ont été violés du fait du traitement de ses données personnelles par la CdCE. Avant d'en arriver là, la CdCE recommande aux personnes concernées de prendre d'abord contact avec:

- le responsable de la sécurité (voir ci-dessus ses coordonnées) et/ou
- le délégué à la protection des données (ECA-Data-Protection@eca.europa.eu, tél. +352 4398-47777).

Les membres du personnel peuvent également demander une évaluation par l'autorité investie du pouvoir de nomination compétente dans leur cas, au titre de l'article 90 du statut du personnel.

12. RÉFÉRENCES

Règlement (CE) n° 45/2001

Lignes directrices du CEPD en matière de vidéosurveillance

Luxembourg, le 19 août 2011
DPO006914FR02-11PP.doc

COUR DES COMPTES EUROPÉENNE
Délégué à la protection des données

Rapport d'audit sur la vidéosurveillance

1. INTRODUCTION

1. Depuis la publication des lignes directrices du CEPD en matière de vidéosurveillance le 17 mars 2010, toutes les institutions de l'UE doivent procéder à un audit de leur infrastructure et de leur politique en matière de vidéosurveillance, ainsi que de leur politique de communication à l'attention des personnes faisant l'objet de cette surveillance.

2. L'audit a été réalisé par M. Johan Van Damme, délégué à la protection des données à la CdCE, et supervisé par M. Meletios Stavrakis, auditeur interne, au cours de la période allant de juin à novembre 2010. Le 11 juin 2010, l'audit a été officiellement notifié au directeur de la direction Finances et soutien (DFS), qui a nommé M. Dimitrios Vavatsis, responsable de la sécurité physique à la CdCE, comme personne de contact au sein de la DFS.

3. Une liste de vérification a été élaborée sur la base des lignes directrices du CEPD en coopération avec le délégué à la protection des données du Parlement européen.

4. Début juin, l'auditeur interne et le délégué à la protection des données ont défini le programme et la méthodologie d'audit et ils ont tenu une première réunion avec le responsable de la sécurité physique le 16 juin 2010. D'autres réunions ont eu lieu les 11 et 30 novembre 2010.

5. L'ensemble de la documentation technique concernant les caméras, le système d'enregistrement et le logiciel a été obtenu auprès du responsable de la sécurité physique au début du mois d'août 2010. Toutes les caméras ont été contrôlées et photographiées.

6. Les principales constatations ont été documentées dans la note d'audit n° 01/2001 établie par l'auditeur interne et adressée au Secrétaire général le 6 janvier 2011 (annexe 1).

7. Le fait que le rapport d'audit du délégué à la protection des données n'a pas été finalisé avant la fin de décembre 2010 – comme le prévoient les lignes directrices – est dû à la cessation du contrat de la société de gardiennage externe, puis à la cessation d'un second contrat passé avec la société externe ayant remplacé la première, et à l'internalisation des activités liées à la sécurité physique à partir du 1er avril 2011. Dès lors, il a fallu réécrire certaines parties de la politique en matière

de vidéosurveillance, modifier les procédures et procéder à une réorganisation du personnel interne qui a abouti à une réattribution des droits d'accès.

2. CHAMP D'APPLICATION ET OBJECTIF

8. L'audit de conformité a exclusivement porté sur les caméras installées et gérées par la CdCE (bâtiments K1, K2 et K8). Les caméras gérées par la Cour de justice ou par *Property Partners* (bâtiment K9) en ont été exclues. Cela est dû au fait que les bâtiments en location ne seront plus utilisés à partir d'octobre 2012, lorsque leurs occupants déménageront dans les locaux de la nouvelle extension – le bâtiment K3.

9. L'audit de conformité a pour objectifs de vérifier dans quelle mesure la CdCE a mis en œuvre les lignes directrices du CEPD en matière de vidéosurveillance, de mettre au jour d'éventuels cas de non-conformité et d'établir un plan d'action, le cas échéant.

3. SYNTHÈSE CONCERNANT LA GESTION

10. Même si elle avait déjà été élaborée pour décembre 2010, la politique en matière de vidéosurveillance n'a toujours pas été adoptée par la CdCE, ni publiée sur les sites intranet/internet.

11. Le système CCTV (télévision en circuit fermé) actuel ne permet pas de crypter le transfert et le stockage des images, ni de conserver un journal (*log*) pour le contrôle du traitement des images stockées.

12. Il n'existe aucune procédure définissant la marche à suivre au cas où des données à caractère personnel seraient divulguées à des personnes non autorisées, ou les mesures à prendre pour avertir ceux dont les données à caractère personnel ont été communiquées.

13. En 2012, au moment de remplacer le système CCTV actuel, il conviendra de spécifier dans l'appel d'offres que le système devra prendre en compte le respect de la vie privée dès la conception (*privacy by design*) et répondre à toutes les exigences techniques propres à ce type de système, telles que définies dans les lignes directrices du CEPD.

4. CONSTATATIONS ET RECOMMANDATIONS

4.1 Prise en compte du respect de la vie privée dès la conception

14. Le système CCTV actuel a été conçu il y a 24 ans et comprend très peu de mesures de protection de la vie privée. Il conviendra de le remplacer pour que toutes les obligations prévues par les lignes directrices puissent être remplies. En 2012, la nouvelle extension du siège de la CdCE, le bâtiment K3, sera prête à accueillir les

membres du personnel qui travaillent actuellement dans les bâtiments loués du K7, du K8 et du K9.

15. Recommandation: En 2012, lorsque le bâtiment K3 sera équipé d'un système de vidéosurveillance conforme aux exigences du CEPD définies dans les lignes directrices, le système CCTV actuel des bâtiments K1 et K2 devra être remplacé par un système compatible avec celui du bâtiment K3.

4.2 Analyse d'impact sur la vie privée

16. Au moment de l'audit, aucune analyse d'impact sur la vie privée n'avait été réalisée en ce qui concerne l'utilisation d'un système CCTV. Une analyse des risques a été effectuée en vue de déterminer si la vidéosurveillance constituait la mesure appropriée pour réduire les risques mis en évidence, mais elle n'a pas été documentée. La note d'audit n° 1 de l'auditeur interne fait état de ces deux constatations. Depuis lors, l'analyse d'impact sur la vie privée a été effectuée et l'analyse des risques documentée.

17. Selon les conclusions de l'analyse d'impact sur la vie privée, l'utilisation de la vidéosurveillance à la CdCE est fondée et son incidence réduite au minimum.

4.3 Information des autorités de protection des données

18. En 2007, il a été notifié au délégué à la protection des données que le personnel et la société de gardiennage externe traitaient des données à caractère personnel obtenues par l'intermédiaire du système de vidéosurveillance.

19. En 2011, l'autorité nationale de protection des données à caractère personnel compétente au Luxembourg a été informée de l'utilisation d'un système de vidéosurveillance couvrant uniquement le site et les bâtiments de la CdCE. Le territoire luxembourgeois n'est pas couvert.

20. Le CEPD en a été informé en vue d'un contrôle préalable en 2011, étant donné que des images pourraient éventuellement être utilisées au cours d'une enquête.

4.4 Décision de recourir à la vidéosurveillance

21. La décision de recourir à la vidéosurveillance a été prise il y a 24 ans, sur recommandation de la direction Sécurité de la Commission. Depuis, l'analyse des risques a montré que la vidéosurveillance constitue la meilleure solution et la plus économique pour prévenir les incidents physiques, protéger les biens et les agents, et garantir la sécurité du personnel dans certains endroits.

22. En ce qui concerne la caméra dans la cage d'escalier du rez-de-chaussée du bâtiment K1, rien ne semble justifier son maintien.

23. Recommandation: Retirer la caméra de la cage d'escalier du rez-de-chaussée du bâtiment K1.

4.5 Communication de la politique en matière de vidéosurveillance

24. La politique, la brochure de synthèse, les avis affichés sur place et les pictogrammes étaient disponibles au moment de l'audit. En revanche, la politique et la brochure de synthèse ne sont pas encore accessibles sur les pages intranet/internet qui leur sont dédiées, puisque la politique n'a pas encore été adoptée.

25. Dans trois cas, les caméras ne sont pas signalées par le pictogramme ISO: aux portes d'entrée menant à la salle des chauffeurs, aux ascenseurs du niveau -1 et au local d'entreposage de la cafétéria.

26. Recommandation: Afficher de manière bien visible le pictogramme ISO signalant le système CCTV aux portes d'accès au local d'entreposage de la cuisine, à la salle des chauffeurs ainsi qu'à la zone regroupant la salle technique et la cantine.

27. Dès son adoption, publier la politique en matière de vidéosurveillance, accompagnée de la brochure de synthèse, sur les pages intranet/internet qui lui sont consacrées.

4.6 Période de conservation

28. La période de conservation des images enregistrées a été fixée à 16 jours pour les bâtiments K1 et K2, et à sept jours pour le bâtiment K8. Cela se justifie par le fait que la CdCE ferme complètement ses portes au cours de la période de Noël et du Nouvel An, et que les responsables de la sécurité physique sont alors indisponibles. Pour que ceux-ci puissent enquêter sur un incident de sécurité physique, les images doivent être conservées pendant une période équivalente à la durée maximale de fermeture de la Cour plus cinq jours ouvrables, afin de permettre la recherche, la copie et/ou le transfert des images.

4.7 Endroits sous surveillance et technologies utilisées

29. Les endroits sous surveillance sont principalement les entrées et les sorties, les portes d'accès, les salles contenant des biens de grande valeur et les endroits où des incidents ont eu lieu. La salle de fitness est la seule exception. L'encadrement supérieur a décidé d'installer cette caméra pour remplacer le surveillant au moment de la cessation du contrat avec la société de gardiennage externe. Les tests ont montré qu'il est parfois possible de reconnaître des personnes à une distance de six mètres de la caméra. Dans tous les autres cas, on peut voir qu'il y a une personne dans la pièce, mais sans qu'il soit possible de l'identifier. Du point de vue du respect de la vie privée, cela est donc acceptable. Toutefois, la raison de sécurité avancée pour justifier l'installation de la caméra est contestable sur le plan de

l'efficacité. L'agent de sécurité devrait pouvoir détecter, dans les meilleurs délais, si une personne dans la salle est en situation de danger; or, ce n'est pas garanti, puisque les agents de sécurité doivent superviser un grand nombre d'autres séquences et s'acquitter d'autres tâches à la réception. L'encadrement supérieur a par ailleurs avancé la réalisation d'une économie de 40 000 euros par an pour justifier l'installation de la caméra.

30. La technologie utilisée est particulièrement respectueuse de la vie privée: il n'y a aucune surveillance dissimulée, le système est autonome, sans interconnexion avec d'autres systèmes d'information; il n'y a ni enregistrement sonore, ni possibilité de zoom ou de suivi; les caméras sont à basse résolution, rendant impossible toute reconnaissance faciale et la fréquence d'enregistrement n'est que d'une image par seconde. Ces constatations sont importantes en ce qui concerne le degré de protection de la vie privée et des données à caractère personnel des gens filmés par le système CCTV.

4.8 Droit d'accès, formation et fonction de journalisation

31. Le système actuel n'autorise l'accès que par l'intermédiaire d'un identifiant générique pour les agents de sécurité. Ce type d'identification ne pose aucun problème, puisque que les agents de sécurité ont seulement accès aux images en temps réel, qu'ils travaillent dans un lieu sécurisé et à accès restreint, inaccessible aux autres membres du personnel, et qu'ils exercent leur tâche de surveillance de manière continue, 24 heures sur 24, sept jours sur sept, 365 jours par an, pour garder les bâtiments et les infrastructures. Un certain nombre d'agents partageant les moniteurs de surveillance, il ne serait ni efficient ni logique qu'ils se connectent au début de chaque nouvelle période de travail avec leur identifiant personnel.

32. Les administrateurs du système partageaient également un identifiant générique. Après la clôture de l'audit, chacun des administrateurs du système a reçu son identifiant personnel.

33. Au moment de la clôture de l'audit, aucune formation spécifique à la protection des données n'était proposée aux utilisateurs du système CCTV. Depuis lors, tous les utilisateurs ont bénéficié d'une formation en janvier et août 2011. Ils ont également tous signé une déclaration spécifique de confidentialité pour protéger les données à caractère personnel auxquelles ils ont accès par l'intermédiaire du système CCTV.

34. Le système n'est pas en mesure de journaliser (*log*) les activités relatives à la recherche, à la copie ou à la suppression des données. La journalisation ne peut être activée qu'au niveau du système d'exploitation pour déterminer à quel moment l'administrateur accède au système.

35. Les images enregistrées ne sont pas cryptées, ce qui protégerait les données au cas où les disques durs contenant ces images seraient volés ou consultés sans supervision adéquate. Dans le cadre du système actuel, il est impossible d'activer le cryptage. Toutefois, les données sont enregistrées dans un format de fichier propriétaire nécessitant un logiciel particulier pour traiter les images.

36. Dans le bâtiment K8, les moniteurs permettant de visionner les images en temps réel à partir des quatre caméras se trouvent dans le bureau du secrétariat de l'unité Logistique. Il s'agit de la meilleure solution possible étant donné que le bail du bâtiment arrive à son terme au cours du dernier trimestre 2012 et qu'aucun emplacement sécurisé n'est disponible. Dans le bâtiment K1, les moniteurs de ce type sont bien situés dans un lieu sécurisé, accessible uniquement au personnel autorisé.

37. Si des images du système CCTV venaient à être communiquées à des personnes non autorisées, il n'existe aucune procédure définissant quand et comment en informer les gens dont les données à caractère personnel ont été divulguées.

38. Recommandation: En 2012, lorsque le bâtiment K3 sera équipé d'un système de vidéosurveillance, le nouveau système devrait pouvoir reconnaître individuellement chaque administrateur du système ainsi que toute personne habilitée à rechercher, à copier et/ou à supprimer des images enregistrées, et permettre de contrôler leurs activités.

39. Le nouveau système devrait permettre le cryptage des images enregistrées.

40. En outre, il convient d'établir une procédure en cas de divulgation d'informations.

4.9 Transfert d'images

41. Le transfert d'images n'est possible que sur avis du délégué à la protection des données. Il n'est autorisé que dans un nombre très limité de cas, dans le cadre d'enquêtes sur des incidents de sécurité ou d'enquêtes disciplinaires ou administratives, ou encore à la demande des services de maintien de l'ordre ou des autorités nationales d'enquête. Les données peuvent également être communiquées à des personnes victimes d'un délit ou de tout autre incident. Tout transfert devra faire l'objet d'une demande écrite préalable qui sera examinée au cas par cas et pourra éventuellement être refusée. Ni l'encadrement supérieur ni les ressources humaines n'ont accès à ces images. Au moment de la clôture de l'audit, il n'existait aucun registre regroupant l'ensemble des transferts, mais il en a été créé un depuis.

4.10 Politique en matière de vidéosurveillance

42. À la fin de l'audit, la politique et la brochure de synthèse correspondante étaient disponibles. Depuis lors, la politique a fait l'objet de plusieurs modifications en raison de l'internalisation de la fonction de responsable de la sécurité physique, ainsi que de nombreux changements d'ordre organisationnel et de la réaffectation de certaines tâches à d'autres unités organisationnelles.

43. Certes, la politique n'avait toujours pas été adoptée à la mi-août, mais les services concernés ont connaissance de son contenu et de son incidence, et la respectent pleinement.

44. Recommandation: La CdCE devrait adopter sans délai la politique en matière de vidéosurveillance pour se conformer aux lignes directrices du CEPD et pour pouvoir en informer le public et toutes les personnes filmées par le système CCTV.

Plan d'action

Action n°	Action	Délai
1	Remplacer le système CCTV actuel lorsque celui du bâtiment K3 sera installé.	1.10.2012
2	Retirer la caméra dans la cage d'escalier du rez-de-chaussée du bâtiment K1.	3.10.2011
3	Afficher trois pictogrammes CCTV dans le garage.	19.9.2011
4	Publier la politique en matière de vidéosurveillance, accompagnée de la brochure de synthèse, sur les pages intranet/internet qui lui sont consacrées.	3.10.2011
5	Établir une procédure en cas de divulgation d'informations.	7.11.2011
6	Adopter la politique en matière de vidéosurveillance.	3.10.2011

COUR DES COMPTES EUROPÉENNE

DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Analyse d'impact sur la vie privée (AIVP)

Vidéosurveillance

(13 juillet 2011)

Vue d'ensemble

La vue d'ensemble doit comprendre les éléments suivants:

- la dénomination technique du système et le nom par lequel il est couramment désigné, ainsi que l'identité de la personne chargée de sa mise en œuvre et de sa surveillance;
- l'objectif du système CCTV;
- une description générale de la technologie et du système:
    - Technologie: par exemple, une description de la caméra et des technologies d'enregistrement, avec les numéros des modèles, les fournisseurs et les fonctions;
    - Système: par exemple, une description des dispositifs du réseau de surveillance, de leur lieu et de leur mode d'implantation, du système de collecte et, le cas échéant, du contrôle des informations visuelles.

Une vue d'ensemble claire et concise fournit au lecteur le contexte dans lequel il doit considérer le reste de l'AIVP.

Le système de vidéosurveillance installé dans les bâtiments K1 et K8, qui date de 1988, a été progressivement étoffé par l'ajout de caméras supplémentaires. Le système de base est un système Geutebrück comprenant neuf caméras à basse résolution, connectées via un réseau type bus, prenant des images en noir et blanc au rythme d'une à la seconde. Il a été complété par un second système Geutebrück, connecté via un réseau IP à un système d'enregistrement d'images Multiscope avec caméras couleur à basse résolution.

Le responsable de la sécurité physique est chargé du système de vidéosurveillance.

La vidéosurveillance au bâtiment K7 relève de la responsabilité de la Cour de justice, étant donné que la CdCE n'est locataire que d'une partie de l'immeuble.

La vidéosurveillance au K9 relève de la responsabilité du propriétaire du bâtiment et est contrôlée par une société privée avec laquelle la CdCE n'entretient aucune relation, contractuelle ou autre.

La vidéosurveillance de l'«Antenne» de Bruxelles relève de la responsabilité du Parlement européen, étant donné que la CdCE n'est locataire que d'une partie du dernier étage.

La vidéosurveillance a pour principal objectif de contrôler l'accès aux locaux et aux bâtiments de la CdCE à des fins de sécurité, et de protéger certains biens de valeur.

Au K1, 15 caméras sont installées: une pour chaque porte extérieure, d'autres autour du bâtiment et à l'entrée du site et une dans la cage d'escalier au rez-de-chaussée.

Au K2, neuf caméras sont installées: une à chaque porte d'entrée, une à la porte d'entrée de la salle informatique, une à l'intérieur de la salle informatique et une dans la salle de fitness.

Au K8, quatre caméras sont installées, une à chaque porte d'entrée extérieure.

Les images des caméras installées dans les bâtiments K1 et K2 sont visualisées en temps réel dans la zone de réception/sécurité du K1, et seuls deux membres du personnel possèdent les droits d'accès permettant de faire des recherches dans les images enregistrées. Le PC permettant d'accéder aux images enregistrées est situé dans une zone sécurisée dont l'accès est limité, et il est protégé par un identifiant et un mot de passe.

Les images des caméras installées au K8 sont visualisées au secrétariat de l'unité Logistique et servent à ouvrir les portes aux visiteurs éventuels. Le PC permettant d'accéder aux images enregistrées est situé dans un local technique verrouillé dont l'accès est limité, et il est protégé par un identifiant et un mot de passe. Aucune image ne peut être extraite.

1 Le Système et les informations collectées et stockées dans celui-ci

Les questions suivantes sont destinées à définir l'ampleur des informations collectées, ainsi que les raisons de leur collecte dans le cadre de la stratégie en cours d'élaboration. Le terme «informations» englobe toutes les images et séquences enregistrées par le système de vidéosurveillance et toutes les informations associées à ces images pouvant être reliées à des personnes. Si les images sont seulement visionnées, mais pas stockées, veuillez l'indiquer ci-après.

1.1 Quelles sont les informations à collecter?

(Veuillez cocher les éléments ci-après s'il y a lieu)
La technologie du système permet:

D'enregistrer une vidéo

Plage statique: entre 3 et 20 mètres
~~Amplitude du zoom:~~
~~Panoramique d'un angle à l'autre~~:

~~D'opérer un suivi~~

~~Automatique (par exemple, déclenché par certains mouvements ou indicateurs)~~
~~Manuel (commandé par un opérateur)~~

~~D'enregistrer le son~~

~~Bande de fréquences:~~

Veuillez décrire ce que la caméra est censée visualiser.

Le système enregistre généralement:

~~Les passants dans la rue.~~
~~Des informations textuelles (telles que les numéros de plaques minéralogiques, les noms de rues et de commerces ou des textes écrits sur les effets personnels des sujets enregistrés).~~
~~Des images normalement inaccessibles à un agent de police dans la rue.~~
~~À l'intérieur de bâtiments commerciaux, de domiciles privés, etc.~~
~~Les étages de bâtiments, de domiciles privés, etc.~~
~~Le système n'enregistre et ne stocke pas les images~~.
Les personnes empruntant les portes d'entrée/des locaux de la CdCE
Les personnes empruntant la cage d'escalier
Les utilisateurs de la salle de fitness
Les visiteurs de la salle informatique

1.1.1 Si l'activité vise à obtenir des informations ou des types d'informations spécifiques, veuillez préciser l'objectif visé.

S.O.

1.1.2 Les informations obtenues par la vidéosurveillance sont-elles associées à d'autres informations; dans l'affirmative, veuillez décrire ces autres informations.

NON

1.2 Sur qui les informations collectées portent-elles?

Le grand public dans les zones contrôlées.
Populations, zones ou activités ciblées (veuillez préciser): utilisateurs de la salle de fitness + visiteurs de la salle informatique
~~Les membres du personnel de sécurité ont pour instruction de cibler des personnes, des activités ou des lieux particuliers.~~

1.2.1 Veuillez décrire toute formation, recommandation ou mesure enjoignant aux agents de sécurité de cibler des personnes, des activités ou des lieux particuliers.

Pendant plusieurs séances, l'attention des agents d'encadrement responsables de la sécurité physique a été attirée sur les lignes directrices du CEPD, sur le fait que la vidéosurveillance peut être très indiscrète, sur les possibilités d'atténuer cette intrusion et sur le fait que des motifs valables doivent être présentés pour pouvoir poursuivre une vidéosurveillance et/ou une vidéosurveillance ciblée.

1.3 Pourquoi les informations sont-elles collectées? Veuillez mentionner toutes les raisons applicables.

~~À des fins de régulation du trafic~~
Prévention de la criminalité
Détection des infractions
Contribution aux enquêtes judiciaires
Reconnaissance des menaces
~~Enquête liée au terrorisme~~
~~Prévention du terrorisme~~
~~Autre (veuillez préciser)~~

1.3.1 Justification de la politique

Veuillez expliquer brièvement pourquoi les caméras sont nécessaires à l'organisation. La description peut porter sur l'un des aspects suivants:

Justification pour la prévention de la criminalité: par exemple: 1) les infractions en cours d'exécution ne peuvent être prévenus que si les images des caméras sont visualisées en temps réel; 2) une caméra clairement visible avertissant le public qu'il est surveillé peut décourager une activité criminelle, à tout le moins dans la zone contrôlée.

Justification pour la contribution aux enquêtes judiciaires: par exemple, une caméra dissimulée peut servir à des fins d'enquête en fournissant après coup des enregistrements de personnes et de lieux, dont la communication peut être ordonnée par le tribunal.

Justification concernant le terrorisme: par exemple, des séquences vidéo sont collectées pour les comparer à des informations contenues dans des bases de données de terroristes.

La première justification concerne le contrôle de l'accès, les agents de sécurité étant chargés d'ouvrir le portail, les portes et le garage; la deuxième concerne la détection d'éventuelles tentatives d'intrusion, la troisième la prévention de la criminalité. Dans la salle de fitness, le but est de s'assurer que des personnes s'entraînant seules n'ont pas été victimes d'un accident ou d'un malaise. En outre,

les caméras sont également destinées à fournir des informations dans le cadre d'une enquête judiciaire.

1.3.2 Veuillez préciser les raisons qui ont motivé le choix de ces caméras en particulier, de leur lieu d'implantation, de ce système de contrôle précis et de ses caractéristiques technologiques. Par exemple, décrivez comment la technologie de prise de vues dans des conditions de faible luminosité a été choisie pour combattre le franchissement illégal d'une frontière la nuit. Il ne suffit pas de mentionner simplement l'objectif général du système.

Le système a été choisi en 1987 lors de la construction du bâtiment principal de la CdCE. Les caméras à basse résolution et le système, facile d'emploi, ont été choisis pour leur excellent rapport qualité/prix et leur robustesse. Ils ont également été choisis de façon à limiter l'impact sur la vie privée (pas d'infrarouge, pas d'enregistrement du son, pas de possibilités de suivi, pas de fonction zoom).

1.3.3 Utilisez-vous les caméras pour suivre et/ou identifier des personnes?

NON

1.4 Comment les informations sont-elles collectées?

~~Contrôle en temps réel, avec défilement des séquences, mais sans stockage.~~
Contrôle en temps réel avec stockage des séquences.
~~Séquences non contrôlées, seulement stockées.~~

1.5 Politiques et procédure d'exploitation

Veuillez décrire les politiques régissant la manière dont les enregistrements peuvent être supprimés, modifiés ou améliorés, aussi bien avant qu'après le stockage. Existe-t-il des politiques de contrôle d'accès définissant qui peut visionner et utiliser les images vidéo et à quelles fins? Existe-t-il des mécanismes de supervision permettant de contrôler qui accède aux enregistrements et de suivre leur utilisation et, dans l'affirmative, ces mécanismes constituent-ils un élément permanent et non modifiable de l'ensemble du système? Quelle formation a été dispensée aux agents contrôlant le système ou ayant accès à celui-ci?

Les enregistrements des images sont effectués de manière cyclique (lorsque le nombre maximal de jours de stockage est atteint, les nouvelles images viennent écraser les anciennes) sur le disque dur du système de vidéosurveillance. Dans le système installé au K8, la capacité du disque dur est tellement limitée que la date de conservation maximale prévue n'a jamais été atteinte. Les images enregistrées ne peuvent être ni modifiées ni améliorées.

Seul le responsable de la sécurité physique (et son adjoint) peut accéder aux images enregistrées. Les conditions d'accès à ces images sont précisées dans la politique de vidéosurveillance.

Des mesures de contrôle permanentes sont mises en œuvre concernant l'utilisation des PC consacrés à l'accès aux images enregistrées, mais le logiciel de visualisation (qui a plus de 23 ans) ne comporte aucun mécanisme de supervision.

L'attention des agents chargés de la sécurité physique ayant accès aux images enregistrées a été attirée par le délégué à la protection des données de la CdCE sur les lignes directrices en matière de vidéosurveillance et sur les principes généraux de la protection des données.

1.6 Efficacité

Décrivez comment l'organisation évalue la performance du système de vidéosurveillance. Des systèmes de mesure spécifiques ont-ils été établis pour l'évaluation? Existe-t-il un calendrier spécifique pour l'évaluation?

Au cours du processus de mise en conformité avec les lignes directrices du CEPD en matière de vidéosurveillance, la CdCE a évalué la performance des systèmes CCTV et recommencera avant de sélectionner le système de vidéosurveillance du nouveau bâtiment, qui devrait être prêt d'ici octobre 2012.

1.7 Comparaison de coûts

L'organisation a-t-elle comparé le coût du système de caméras avec celui d'autres moyens d'attendre les objectifs du système, qui pourraient avoir un impact moindre sur la vie privée? Dans l'affirmative, veuillez présenter une synthèse de cette comparaison des coûts (par exemple, comparez le coût du système de caméras et celui du recrutement d'agents de sécurité supplémentaires pour patrouiller dans la zone.)

Oui, nous avons effectivement procédé à cette comparaison et les systèmes CCTV actuels ont coûté 0 € (zéro euro) à la CdCE depuis leur installation. Si ces caméras devaient être remplacées par des agents de sécurité chargés de vérifier, à chaque fois qu'une personne se présente à une porte d'entrée, si celle-ci représente une menace potentielle, il faudrait recruter huit agents de sécurité supplémentaires, ce qui représente un coût de 40 000 euros par an et par agent.

1.8 Quelles sont les autorités, dispositions et/ou conventions légales qui régissent le système de caméras?

Cette rubrique doit comprendre une description de l'autorisation législative accordée aux institutions, aux agences et aux organes de l'UE, ainsi que de toute décision exécutive ou répressive autorisant la mise en place du système. Veuillez également fournir une liste des restrictions ou des règlements régissant l'utilisation du système de caméras. Il peut s'agir de normes en vigueur en matière d'application de la loi, telles que des citations à comparaître et des mandats, ou encore de règles spécifiques à la surveillance. Par exemple, un mandat est-il requis pour suivre ou identifier une personne?

Règlement (CE) n ° 45/2001
Lignes directrices du CEPD en matière de vidéosurveillance
Le CEPD est l'autorité de contrôle.
Le délégué à la protection des données de la CdCE réalise un audit annuel du système de vidéosurveillance.

1.9 Le processus décisionnel

Veuillez décrire le processus décisionnel ayant conduit à l'acquisition du système de caméras.
Le processus décisionnel a inclus des commentaires ou des examens publics.
Le processus a été fondé sur:

- ~~des études de cas~~
- ~~des travaux de recherche~~
- ~~des auditions~~
- ~~des recommandations de fournisseurs de caméras~~
- ~~des informations provenant d'autres sources~~

autre (veuillez préciser)

La direction de la sécurité de la Commission européenne a été consultée en 1987 afin de déterminer quel système de CCTV convenait au bâtiment de la CdCE.

1.10 Analyse d'impact sur la vie privée

Compte tenu du volume et du type de données collectées, ainsi que de la structure, de la finalité et de l'utilisation du système, veuillez indiquer quels sont les risques pour la vie privée qui ont été mis en évidence et comment ils ont été atténués. Si, au cours du processus de conception du système ou de sélection du type de technologie, des décisions ont été prises pour limiter la portée de la surveillance ou augmenter l'obligation de rendre compte, veuillez joindre un exposé de ces décisions.
Parmi les risques importants pour la vie privée, vous pouvez notamment décrire ceux qui concernent:

- **les droits à la vie privée**. Par exemple, les caméras peuvent filmer des personnes pénétrant dans certains lieux ou se livrant à certaines activités, dans des circonstances où ces personnes ne s'attendent pas à être identifiées ou suivies. Il peut s'agir d'une visite à un cabinet médical ou encore de la présence à une réunion d'alcooliques anonymes ou à un rassemblement social, politique ou religieux;
- **la liberté de parole et d'association**. Les caméras peuvent fournir au gouvernement des enregistrements de ce que des personnes déclarent, font et lisent dans la sphère publique, par exemple en filmant des personnes présentes à un rassemblement donné ou en établissant l'existence d'associations entre certaines personnes. Ce genre d'enregistrement peut avoir pour effet d'entraver la liberté d'expression et d'association garantie par la constitution;
- **l'obligation de rendre compte du gouvernement et les garanties procédurales**. Bien que l'on puisse s'attendre à ce que les personnes chargées du maintien de l'ordre et les autres agents habilités utilisent la technologie de façon légitime, les concepteurs du système doivent anticiper les utilisations non autorisées et prévoir des garde-fous contre celles-ci, y compris la création d'un système obligeant à rendre compte de toutes les utilisations;
- **l'égalité de protection et la discrimination**. La surveillance exercée par le gouvernement, du fait que celui-ci se livre à certaines activités de surveillance policière invisibles pour le public, est associée à des risques accrus d'abus, tels que l'établissement d'un profil sur la base de la race, de la citoyenneté, du sexe, de l'âge, du niveau socioéconomique, de l'orientation sexuelle ou d'autres critères. Les décisions relatives à la mise en place de caméras et les décisions ad hoc concernant leur utilisation devraient être le produit de processus et de réflexions rationnels et non discriminatoires. Les décisions relatives au système devraient être examinées dans un esprit d'équité et de non-discrimination.

  Chaque caméra prend uniquement des images à basse résolution, sauvegardées à la fréquence d'une image par seconde. Ces images enregistrées ne sont accessibles qu'à partir d'un PC situé dans une zone sécurisée, lui-même protégé par un identifiant et un mot de passe. Prière de se reporter au point 1.3.1 pour la finalité et l'utilisation de la vidéosurveillance.

  Le seul impact sur la vie privée à avoir été constaté concerne la caméra installée dans la salle de fitness, qui permet d'identifier les personnes qui s'entraînent à 5 mètres au plus de la caméra. Le comité du personnel s'est enquis du bien-fondé de cette caméra et a demandé si la présence à temps plein d'un entraîneur de fitness ou d'un agent de sécurité ne constituerait pas une meilleure solution.

2 – Utilisations du système et des informations

2.1 Veuillez décrire les utilisations des séquences ou des images fournies par les caméras.

Veuillez décrire en détail comment les séquences ou les images sont utilisées, et comment elles pourraient l'être à l'avenir.

Entre 3 et 20 mètres, et de la manière décrite au point 1.3.1.

Aucune modification n'est prévue à l'avenir.

2.2 Analyse d'impact sur la vie privée

Veuillez décrire tous les types de contrôle en place afin de garantir que les séquences ou les images sont traitées conformément aux utilisations décrites ci-dessus. Par exemple, l'utilisation appropriée des informations est-elle abordée dans la formation dispensée à tous les utilisateurs du système? Les journaux de contrôle sont-ils examinés régulièrement? Quelles sont les mesures disciplinaires en vigueur s'il est constaté qu'une personne utilise la technologie ou les enregistrements de manière inappropriée?

Seuls deux utilisateurs ont accès au système. Les fichiers journaux sont contrôlés une fois par an ou en cas d'incident, ou encore en cas de doute concernant l'utilisation appropriée du système.

Les mesures disciplinaires applicables en cas d'utilisation ou de divulgation à des fins inappropriées, d'informations obtenues par le fonctionnaire dans l'exercice de ses fonctions sont précisées dans le statut.

3 – Conservation

Les questions ci-après sont destinées à définir la durée pendant laquelle les informations sont conservées après leur collecte initiale.

3.1 Quelle est la période de conservation des informations dans le système? (Autrement dit, pendant combien de temps les séquences ou les images sont-elles stockées?)

~~Entre 24 et 72 heures~~
~~Entre 72 heures et une semaine~~
~~Entre une semaine et un mois~~
~~Entre un et trois mois~~
~~Entre trois et six mois~~
~~Entre six mois et un an~~
~~Plus d'un an (veuillez préciser)~~
~~Indéfiniment~~
16 jours, afin de pouvoir couvrir la période maximale de fermeture de la CdCE (Noël et Nouvel An) + 5 jours ouvrables.

3.1.1 Décrivez les dérogations éventuelles à la période de conservation (par exemple, dans le cadre d'une enquête ou d'un examen)

Au cours d'une enquête administrative ou disciplinaire, les images concernant les éléments faisant l'objet de l'enquête peuvent être conservées pendant tout le déroulement de la procédure, ainsi que pendant la période prévue pour l'appel.

3.2 Procédure de conservation

Les séquences ou les images sont automatiquement effacées après l'expiration de la période de conservation
~~L'effacement exige l'intervention d'un opérateur système~~
~~Dans certaines circonstances, les agents peuvent outrepasser la période de conservation:~~
~~pour supprimer les séquences ou les images avant la fin de la période de conservation~~
~~pour conserver les séquences ou les images au-delà de la période de conservation~~
~~Veuillez décrire les circonstances et le processus officiel permettant d'outrepasser la période de conservation~~

3.3 Analyse d'impact sur la vie privée:

Étant donné la finalité de la conservation des informations, veuillez expliquer pourquoi elles sont conservées pendant la période indiquée.

La période de conservation de 16 jours est destinée à laisser le temps aux agents responsables de la sécurité physique ayant accès aux images enregistrées de revisionner un incident. La CdCE étant fermée entre Noël et Nouvel An, ces agents ne sont pas présents à la Cour pendant ce laps de temps. Cette période a été prolongée de 5 jours ouvrables supplémentaires afin de permettre aux agents responsables de la sécurité physique d'accéder aux images enregistrées.

4 – Partage et divulgation en interne

Les questions ci-après sont destinées à établir l'ampleur du partage *au sein* de l'organisation. *Le partage externe avec des entités étrangères à l'organisation est abordé dans la rubrique suivante.*

4.1 Avec quelles entités internes et quelles catégories de personnel les informations sont-elles partagées?

Entités internes
~~Enquêteurs~~
~~Unité d'audit interne~~
~~Unité financière~~
~~Unité de sécurité physique~~
~~Autre (veuillez préciser)~~
~~Aucune~~

~~Catégories de personnel~~
~~Personnel de direction (veuillez préciser quels postes)~~
~~Encadrement moyen (veuillez préciser)~~
~~Employés subalternes~~
~~Autre (veuillez préciser)~~

4.2 Pour les entités internes énumérées ci-dessus, quelle est l'étendue de l'accès qui leur est octroyé? (En d'autres termes, à quels enregistrements et à quelle technologie ont-elles accès et dans quel but?)

En présence du responsable de la sécurité physique, elles peuvent rechercher, visionner, extraire et, le cas échéant, imprimer les images.

4.2.1 Existe-t-il une politique écrite régissant la manière dont l'accès est octroyé?

~~Non~~
Oui (veuillez préciser)
Modalités établies dans la politique en matière de vidéosurveillance

4.2.2 L'octroi de l'accès est-il spécifiquement autorisé par:

~~Un statut (veuillez préciser lequel)~~
~~Un règlement (veuillez préciser lequel)~~
Autre (veuillez préciser): procédures d'enquête.
~~Rien~~

4.3 Comment les informations sont-elles partagées?

4.3.1 Le personnel disposant d'un droit d'accès peut-il obtenir les informations:

~~Depuis l'extérieur, à partir d'un serveur distant~~
Via des copies de la vidéo distribuées à ceux qui en ont besoin
Uniquement en visionnant la vidéo sur place
Autre (veuillez préciser): voir point 4.2

4.4 Analyse d'impact sur la vie privée:

Eu égard à l'étendue du partage d'informations en interne, veuillez indiquer quels sont les risques pour la vie privée qui ont été mis en évidence et comment ils ont été atténués. Par exemple, veuillez mentionner les contrôles d'accès, les systèmes de cryptage, la formation, les règlements ou les procédures disciplinaires qui garantissent une utilisation strictement légitime du système au sein du département.

Les informations recueillies dans le cadre d'enquêtes sont toujours traitées avec le niveau de sécurité et de confidentialité le plus élevé possible, mises sous clef dans des endroits sécurisés et traitées sur des PC non connectés au réseau. Aucune formation n'a été dispensée aux personnes chargées des enquêtes.

5 – Partage et divulgation à l'extérieur

Les questions ci-après sont destinées à définir le contenu des informations et l'ampleur de leur partage, ainsi que l'autorité responsable de celui-ci à l'extérieur de votre organisation – par exemple, un autre organe de l'UE, une agence ou instance nationale, ou encore une entité privée ou un particulier.

5.1 Avec quelles entités externes les informations sont-elles partagées?

Veuillez indiquer le nom des entités externes avec lesquelles les séquences ou les images, ainsi que les informations connexes, sont partagées. Par «entités externes», il faut entendre les particuliers ou les groupes extérieurs à votre organisation.

~~Agences gouvernementales locales (veuillez préciser)~~
~~Agences nationales (veuillez préciser)~~
~~Organes de l'UE (veuillez préciser)~~
~~Entités privées:~~
~~Entreprises situées dans des zones contrôlées~~
~~Compagnies d'assurance~~
~~Médias~~
Autre (veuillez préciser). Si un délit était commis et que la preuve de celui-ci figurait sur les images enregistrées ou si celles-ci permettaient d'identifier les auteurs des méfaits, elles pourraient être remises aux forces de l'ordre nationales.
Particuliers:
~~Victimes d'infractions~~
~~Prévenus~~
~~Parties civiles~~
~~Grand public~~
~~Autre (veuillez préciser)~~

5.2 Quelles sont les informations partagées et à quelles fins?

5.2.1 Pour chaque entité ou personne mentionnée ci-dessus, veuillez indiquer tous les éléments suivants:

La finalité de la divulgation: enquêtes judiciaires
La réglementation régissant la divulgation: sur présentation d'un mandat délivré par le procureur général de l'État
Les conditions dans lesquelles les informations ne sont pas divulguées: sans objet, mais voir point 5.3
Citations à comparaître devant une autorité spécifique autorisant le partage des séquences ou des images des caméras: S.O.

5.3 Comment les informations sont-elles transmises ou divulguées aux entités externes?

Des images ou des séquences discontinues enregistrées par les caméras sont partagées au cas par cas
~~Certaines entités externes ont un accès direct aux séquences ou aux images enregistrées par les caméras~~
~~Flux en temps réel de séquences ou d'images entre des agences ou des services~~
~~Les séquences ou les images sont transmises sans fil ou téléchargées à partir d'un serveur~~
~~Les séquences ou les images sont transmises sur papier~~
~~Les séquences ou les images ne sont accessibles que sur place~~

5.4 Existe-t-il un protocole d'accord (PA), un contrat ou une convention avec chaque organisation externe avec laquelle

les informations sont partagées et le PA fait-il apparaître la portée des informations actuellement partagées?

~~Oui~~
Non

S'il n'existe pas de PA, veuillez décrire les mesures prises pour remédier à cette lacune.
Les forces de police doivent respecter un protocole strict lorsqu'elles pénètrent dans les institutions de l'UE et, pour obtenir des informations, elles doivent présenter une demande officielle émanant d'un procureur.

5.5 Comment les informations partagées sont-elles sécurisées par le destinataire?

Pour chaque interface avec un système situé à l'extérieur de votre organisation:
~~Il existe une politique écrite définissant comment garantir la sécurité lors du partage d'informations~~
~~Une personne est chargée de veiller au maintien de la sécurité du système lors du partage d'informations (veuillez préciser)~~
~~L'entité externe a le droit de divulguer à son tour les informations à d'autres entités~~
~~L'entité externe n'a pas le droit de divulguer à son tour les informations à d'autres entités~~
~~Les protections technologiques telles que le verrouillage, le floutage des visages ou le suivi de l'accès restent activées une fois que les informations ont été communiquées~~
~~Les protections technologiques ne restent pas activées une fois que les informations ont été communiquées~~
La police luxembourgeoise a ses propres règles strictes concernant la nature des informations pouvant être divulguées.

5.6 Analyse d'impact sur la vie privée:

En cas de partage externe, quels sont les risques pour la vie privée qui ont été mis en évidence? Veuillez décrire comment ils ont été atténués. Par exemple, s'il existe une convention en matière de partage, quels sont les garde-fous (notamment formation, contrôle d'accès ou garantie de la protection de la vie privée par des moyens technologiques) qui ont été mis en œuvre pour garantir que les informations soient utilisées correctement par des agents extérieurs?

Cela est du ressort de la police.

6 – Accès technique et sécurité

6.1 Qui est en mesure d'effacer, de modifier ou d'améliorer des enregistrements aussi bien avant qu'après le stockage?

~~Personnel d'exploitation~~
~~Personnes ayant un accès systématique ou permanent au système (veuillez préciser)~~
Autre (~~veuillez préciser~~): En principe, il n'est pas possible d'effacer, de modifier ou d'améliorer les enregistrements.

6.1.1 Différents niveaux d'accès sont-ils octroyés en fonction du poste de l'utilisateur? Dans l'affirmative, veuillez fournir des détails.

~~Tous les utilisateurs autorisés ont accès en temps réel aux séquences ou aux images~~
~~Seuls certains utilisateurs autorisés ont accès en temps réel aux séquences ou aux images (veuillez préciser lesquels)~~
~~Tous les utilisateurs autorisés ont accès aux séquences ou aux images stockées~~
~~Seuls certains utilisateurs autorisés ont accès aux séquences ou aux images stockées (veuillez préciser lesquels)~~
~~Tous les utilisateurs autorisés peuvent commander les fonctions de la caméra (panoramique, inclinaison, zoom)~~
~~Seuls certains utilisateurs peuvent commander les fonctions de la caméra~~
~~Tous les utilisateurs autorisés peuvent effacer ou modifier des séquences ou des images~~
~~Seuls certains utilisateurs autorisés peuvent effacer ou modifier des séquences ou des images (veuillez préciser lesquels)~~
Seuls les agents de sécurité peuvent visualiser les images en temps réel.
Seules deux personnes peuvent accéder aux images enregistrées.

6.1.2 Existe-t-il des procédures écrites réglementant l'octroi de l'accès à des utilisateurs pour la première fois?

~~Oui (veuillez préciser)~~
Non

6.1.3 Quand l'accès est octroyé:

~~Il existe des moyens de limiter l'accès aux enregistrements ou à la technologie concernés (veuillez préciser)~~
Il n'existe aucun moyen de limiter l'accès

6.1.4 Existe-t-il des mécanismes d'audit?

~~Pour contrôler qui accède aux enregistrements?~~
~~Pour suivre leur utilisation?~~

6.1.5 La formation reçue par les utilisateurs potentiels comprend l'étude des:

Questions de responsabilité
Questions de vie privée
Aspects techniques du système
Limites des utilisations du système
Procédures disciplinaires
~~Autre (veuillez préciser)~~
~~Pas de formation~~

La formation dure:

~~Aucune~~
De 0 à 1 heure

~~De 1 à 5 heures~~
~~De 5 à 10 heures~~
~~De 10 à 40 heures~~
~~De 40 à 80 heures~~
~~Plus de 80 heures~~

La formation consiste en:

~~Un cours~~
~~Une vidéo~~
~~Des documents écrits~~
~~Des documents écrits, mais pas d'instruction verbale~~
~~Néant~~
Autre (veuillez préciser): Brèves présentations des règlements suivies de séances de questions-réponses.

6.2 Le système est audité:

~~Lorsqu'un employé possédant un accès quitte l'organisation~~
Si un employé fait l'objet d'une mesure disciplinaire suite à une utilisation incorrecte du système
~~Une fois par semaine~~
~~Une fois par mois~~
Une fois par an
~~Jamais~~
En cas de besoin

6.2.1 L'audit du système est:

Réalisé par une personne appartenant à l'organisation: le délégué à la protection des données
~~Réalisé par une personne extérieure à l'organisation~~
Supervisé par un organe extérieur (par exemple, un conseil municipal ou un autre organe élu – veuillez préciser): le CEPD

6.3 Analyse d'impact sur la vie privée:

Eu égard à la sensibilité et à la portée des informations collectées, quels sont les risques en matière de vie privée liés à la sécurité qui ont été mis en évidence et atténués?

Le seul risque en matière de vie privée qui ait été mis en évidence est le fait que les images enregistrées par la caméra installée dans la salle de fitness, qui permet d'identifier les personnes qui s'entraînent à 5 mètres au plus de la caméra, pourraient être utilisées pour épier ces sportifs enthousiastes.

Le risque a été considéré comme acceptable par l'encadrement supérieur.

7 – Avis

7.1 Les sujets susceptibles d'être enregistrés par une caméra sont-ils avertis qu'ils se trouvent dans le champ d'une caméra?

Des panneaux disposés dans les espaces publics avisent les personnes qui s'y trouvent qu'elles sont filmées par des caméras

Avis dans plusieurs langues
Une copie de cet avis est jointe en annexe:
«Pour votre sécurité, ce bâtiment et son voisinage immédiat sont placés sous vidéosurveillance. Les images sont conservées pendant 16 jours. Pour de plus amples informations, veuillez consulter la page eca.europa.eu/cctv ou prendre contact avec l'unité de sécurité de la CdCE en téléphonant au +352 4398-1 ou en adressant un courriel à ECA-security@eca.europa.eu»
~~Pas d'avertissement~~
~~Autre (veuillez préciser)~~

8 – Technologie

Les questions suivantes ont pour objet d'analyser le processus de sélection de toute technologie utilisée par le système de vidéosurveillance, comprenant les caméras, les objectifs, ainsi que le matériel d'enregistrement et de stockage.

8.1 Des technologies concurrentes ont-elles été évaluées afin de comparer leur capacité à atteindre les objectifs du système, y compris la protection de la vie privée?

Oui
~~Non~~

8.2 Quels sont les choix en matière de conception qui ont été opérés afin de renforcer le respect de la vie privée?

~~Le système comprend une technologie de floutage des visages~~
~~Le système comprend une technologie de verrouillage~~
~~Les lieux d'implantation des caméras font l'objet de restrictions afin de respecter la vie privée~~
Le système est doté d'une autre technologie renforçant le respect de la vie privée (veuillez préciser)
Images stockées avec une basse résolution
Pas de possibilité de zoom ni de suivi, caméras fixes, en noir et blanc pour la plupart
Seulement stockage image par image toutes les secondes
~~Aucun (veuillez préciser)~~

9 – Annexes à l'AIVP

~~Législation en matière d'autorisation~~
~~Documents d'octroi~~
~~Transcription d'une audition publique ou d'une session parlementaire~~
~~Manuels de programmes décrivant les règles et règlements applicables au système~~
~~Autre (veuillez préciser)~~

Signature du responsable de la sécurité physique

Dimitrios Vavatsis

Signature du délégué à la protection des données

Johan Van Damme

_____

To be filled out in the EDPS' office

NUMERO DE REGISTRE:

NOTIFICATION DE CONTRÔLE PREALABLE

Date de soumission :

Numéro de dossier :

Institution :

Base légale : article 27-5 du Règlement CE 45/2001(1)

(1) OJ L 8, 12.01.2001

INFORMATIONS NECESSAIRES (2)

(2) Merci de joindre tout document utile

1/ Nom et adresse du responsable du traitement
Cour des comptes européenne
12 rue Alcide de Gasperi
L-1615 Luxembourg

2/ Services de l'institution ou de l'organe chargés du traitement de données à caractère personnel
Cellule sécurité physique & réception - Unité Logistique - Direction Finances et Soutien

3/ Intitulé du traitement
Vidéosurveillance

4/ La ou les finalités du traitement
Contrôle d'accès des bâtiments et certaines locaux
Prévention à l'intrusion et criminalité
Protection des biens et personnes
Comme outil dans la sauvegarde des gens victime d'un indicent ou malaise à la salle du fitness.
Utilisé comme une preuve éventuelle aux cour des investigations.

5/ Description de la catégorie ou des catégories de personnes concernées
Des gens qui entrent et quittent des bâtiments.
Certaines utilisateurs de la salle de fitness
Des gens qui entrent dans la salle des serveurs.

6/ Description des données ou des catégories de données *(en incluant, si nécessaire, les catégories particulières de données (article 10) et/ou l'origine des données)*

Images des gens et voitures qui entrent et sortent le site et/ou les bâtiments ainsi la salle des serveurs et certaines utilisateurs de la salle fitness.

7/ Informations destinées aux personnes concernées

Pictogrammes à l'entrée du site et à plusieurs portes, notification en 3 langues (FR, DE, EN) à chaque entrée des bâtiments, politique de vidéosurveillance disponible sur Intranet/Internet de la Cour.

8/ Procédures garantissant les droits des personnes concernées*(droits d'accès, de faire rectifier, de faire verrouiller, de faire effacer, d'opposition)*

Les personnes filmées peuvent faire une demande auprès la sécurité physique ou le DPO pour consulter les images auxquelles ils se trouvent.
Il n'y a pas moyen de demander la rectification, le verrouillage, l'effacement des images ou faire opposition d'être filmé (sauf à ne pas entrer aux endroits qui sont couvert par les cameras).

9/ Procédures de traitement automatisées / manuelles
Le traitement est entièrement automatisé: du capture jusqu'au effacement des images.

10/ Support de stockage des données
Les images sont stockées en format digitalisé sur les disques durs du PC/enregistreur.

11/ Base légale et licéité du traitement

Décision du management en 1988 d'installer un système de vidéosurveillance au bâtiment de la Cour
Politique de vidéosurveillance.

12/ Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être

Responsables pour la sécurité physique et gardiens de sécurité.
Police au autre services d'investigations.
Les personnes victime d'un incident physique ou d'une crime.
Des investigateurs des investigations administratives/disciplinaires

13/ Politique de conservation des données personnelles (ou catégories de données)

Les images sont sauvegardé 16 jours au bâtiment principal (K1 & K2) et sept jours au bâtiment K8.

13 a/ Dates limites pour le verrouillage et l'effacement des différentes catégories de données
(après requête légitime de la personne concernée)
(Merci d'indiquer les dates limites pour chaque catégorie, si nécessaire)

N/A

14/ Finalités historiques, statistiques ou scientifiques
Si vous conservez les données pour des périodes plus longues que celles mentionnées ci-dessus, merci d'indiquer, si nécessaire, ce pourquoi les données doivent être conservées sous une forme permettant l'identification.

N/A

15/ Transferts de données envisagés à destination de pays tiers ou d'organisations internationales

N/A

16/ Le traitement présente des risques particuliers qui justifient un contrôle préalable :(Merci de décrire le traitement):

Comme spécifié dand les lignes directrices du CEPD un contrôle préalable est nécessaire au moment que les images peuvent être utilisés pendants une investigation ne pas causé par un incident physique.

comme prévu à:

XArticle 27.2.(a)
Les traitements de données relatives à la santé et les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté,

Article 27.2.(b)
Les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement,

□ Article 27.2.(c)

L*es traitements permettant des interconnexions non prévues en vertu de la législation nationale ou communautaire entre des données traitées pour des finalités différentes,*

□ Article 27.2.(d)

Les traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat,

□ Autre (concept général de l'article 27.1)

17/ Commentaires

18/ Mesures prises pour assurer la sécurité du traitement *(3)*
Merci de vérifier tous les points de l'article 22 du règlement (CE) 45/2001.
3) Ne sera pas publié dans le registre du CEPD (article 27.5 du règlement (CE) 45/2001)

LIEU ET DATE: Luxembourg 08/08/2011

DELEGUE A LA PROTECTION DES DONNEES: Johan VAN DAMME

INSTITUTION OU ORGANE COMMUNAUTAIRE: Cour des comptes européenne

To be filled out in the EDPS' office

AVIS DU CEPD

Suivi *(en cas de mesures à prendre)*

VIDÉOSURVEILLANCE

Pour votre sécurité, ce bâtiment et son voisinage immédiat sont placés sous vidéosurveillance. Les images sont conservées pendant 16 jours.

Pour de plus amples informations, veuillez consulter la page eca.europa.eu/cctv ou prendre contact avec l'unité de sécurité de la CdCE en téléphonant au +352 4398 1 ou en adressant un courriel à

ECA-security@eca.europa.eu.

Les badges doivent être portés de manière visible

VIDEOÜBERWACHUNG

Zu Ihrer Sicherheit werden dieses Gebäude und seine unmittelbare Umgebung videoüberwacht. Die Aufnahmen werden 16 Tage lang gespeichert.

Weitere Auskünfte erhalten Sie unter der Adresse www.eca.europa.eu/cctv.

Sie können sich aber auch mit der Sicherheitsabteilung des ERH unter +352 4398 1 oder

ECA-security@eca.europa.eu

in Verbindung setzen.

Ausweise müssen sichtbar getragen werden

VIDEO SURVEILLANCE

For your safety and security, this building and its immediate vicinity is under video-surveillance. Recordings are retained for 16 days.

For further information, please consult eca.europa.eu/cctv or contact the ECA's security unit at +352 4398 1 or ECA-security@eca.europa.eu.

Badges must be worn visibly