Direction générale des infrastructures

Politique de vidéosurveillance

Cour de justice de l'Union européenne

TABLE DES MATIERES

1. Objectif et champ d'application de la politique de vidéosurveillance de l'Institution

Le 5 juillet 2005, la commission « Bâtiments » de la Cour de justice de l'Union européenne a pris acte du *Schéma directeur de mise en sûreté globale du complexe immobilier de la Cour de Justice des Communautés Européennes*.

Parmi les différentes recommandations de cette étude, figurait l'installation d'un système de vidéosurveillance afin d'assurer la sécurité des bâtiments, des biens et des personnes.

L'Institution a dès lors mis en place un système de vidéosurveillance. L'état de la situation sur l'exploitation du système de vidéosurveillance a été présenté au Comité Administratif, qui en a pris acte au cours de sa réunion du 1er juillet 2009.

Le présent document décrit le système de vidéosurveillance dans son état actuel et les mesures prises par l'Institution afin de protéger les données à caractère personnel, le droit à la vie privée et les autres droits fondamentaux.

2. Respect de la vie privée, protection des données et conformité du système de vidéosurveillance

2.1 Révision du système existant

La Cour de justice de l'Union européenne exploitait un système de vidéosurveillance avant que les lignes directrices du Contrôleur européen de la protection des données (ci-après "CEPD") en matière de vidéosurveillance du 17 mars 2010 (ci-après les "lignes directrices") soient publiées.

Le système de vidéosurveillance et les procédures de l'Institution ont été mis en conformité vis-à-vis de la législation en matière de protection des données à caractère personnel et plus particulièrement avec les recommandations du CEPD reprises dans les lignes directrices[1].

2.2 Statut de conformité

La Cour de justice de l'Union européenne traite les images en conformité avec le règlement (CE) N° 45/2001 du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (ci-après, le "règlement n° 45/2001"), et avec les lignes directrices.

[1] Les lignes directrices en matière de vidéosurveillance sont disponibles sur le site internet du CEPD :

https://secure.edps.europa.eu/EDPSWEB/edps/lang/fr/Supervision/Guidelines

2.3 Audit interne

Un audit interne sera réalisé tous les 2 ans.

2.4 Information sur le statut de conformité au CEPD

Le traitement des données à caractère personnel inhérent au système de vidéosurveillance a été notifié au CEPD une première fois en avril 2009.
Suite à l'adoption de la présente politique de vidéosurveillance, la Cour de justice de l'Union européenne a notifié l'état de conformité au CEPD en lui adressant un exemplaire du présent document.

2.5 Contact avec l'autorité compétente de la protection des données de l'Etat membre

L'autorité compétente de la protection des données au Luxembourg (Commission nationale pour la protection des données - CNPD) a été informée en novembre 2006. Ses remarques et recommandations[2] ont été prises en compte.

2.6 Transparence

La politique de vidéosurveillance est accessible :

- sur le site intranet de la Section sécurité et sûreté : http://intranet/infrastructures/indispensables/securite.htm
- sur le site intranet du délégué à la protection des données : http://intranet/dpo/FR/Home_FR.htm
- sur le site web de la Cour de justice de l'Union européenne à l'adresse suivante :
- http://curia.europa.eu/jcms/jcms/P_127468 : L'institution > Se rendre à la Cour > Conditions générales.

2.7 Contrôles périodiques

La Section sécurité et sûreté de l'Institution procédera tous les deux ans à un contrôle en matière de protection des données. Lors de ces contrôles périodiques, une analyse sera faite s'agissant de :

- la nécessité de disposer d'un système de vidéosurveillance ;
- la concordance du système avec les objectifs préposés ;
- l'absence d'alternatives adéquates.

Les contrôles périodiques viseront notamment à vérifier si la politique de vidéosurveillance de la Cour de justice de l'Union européenne reste conforme au règlement n° 45/2001 et aux lignes directrices (audit d'adéquation) et si cette politique est respectée en pratique (audit de conformité).

[2] En particulier dans une lettre du 15/03/2014 adressée au responsable du traitement, la CNPD, a indiqué que « *seul le règlement n° 45/2001 trouvera application, dès lors que le système de vidéosurveillance (…) se limitera strictement au domaine privé, en excluant toute surveillance du domaine public* ».

2.8 Solutions techniques favorisant le respect de la vie privée

La Cour de justice de l'Union européenne a implémenté les solutions technologiques respectueuses de la vie privée suivantes :

- Les angles de vue et les objectifs des caméras ont été choisis pour couvrir uniquement les zones à surveiller ;
- Les zones des bâtiments pour lesquels les attentes en matière de respect de la vie privée sont encore plus élevées ne sont pas surveillées par des caméras ;
- Un logiciel spécifique, un profil utilisateur et un mot de passe sont nécessaires pour que les personnes autorisées, à savoir un petit nombre de membres de la Section sécurité et sûreté, puissent accéder aux images enregistrées ;
- Toutes les manipulations sur le système sont enregistrées (enregistrement de l'action et de l'utilisateur qui l'a réalisée).

3. Endroits sous surveillance

Conformément au Schéma directeur de sûreté, un système de vidéosurveillance qui compte 526 caméras a été installé sur le site actuel (surface voisine de 220 000 m²).

Le système de vidéosurveillance couvre :

- Abords extérieurs / Issues de secours
  Objectif : dissuasion de toute tentative d'intrusion ou d'incivilités

- Accès aux réceptions
  Objectif : surveillance des flux d'entrée et de sortie

- Accès parkings (barrières et portes) / Rampes et chemins de circulation dans les différents niveaux des parkings
  Objectif : dissuasion de dégradations aux biens de l'Institution, atteintes aux personnes et aide à la résolution de différends à cet égard

- Quais de livraison et rue technique
  Objectif : surveillance des livraisons et des accès entre quais de livraison et rue technique, protection des installations techniques sensibles

- Zones publiques à l'intérieur des bâtiments
  Objectif : observation par le Poste de Commandement et de Sécurité de la situation générale afin de réagir en cas d'événement (troubles de l'ordre, objet suspect abandonné, chute de personne, etc.) ; surveillance des œuvres d'art ; intervention rapide en cas d'incendie ou en cas de malaise.

- Passages vers les zones privatives protégées
  Objectif : prévention de toute tentative d'intrusion illicite dans ces zones et apporter, conjointement avec le système de parlophonie, l'aide nécessaire aux utilisateurs en cas de difficulté avec les équipements de contrôle d'accès (portiques de contrôle unicitaire ou lecteurs de badges).

Des plans avec les implantations des caméras sont disponibles auprès de la Section sécurité et sûreté de l'Institution et accessibles à celle-ci. Ces plans sont accessibles, sur demande, au responsable du traitement des données, au Délégué à la protection des données de l'Institution (ci-après « DPD ») et au CEPD.

Aucune caméra n'est dirigée sur les endroits où les personnes peuvent s'attendre à un respect plus important de leur vie privée.

4. Informations personnelles recueillies et motif de leur collecte

4.1 Description sommaire et spécifications techniques détaillées du système

Le système de vidéosurveillance enregistre des images dans un format numérique et est équipé d'un système de détection de mouvement. Le système enregistre les mouvements détectés par les caméras dans les zones de surveillance ainsi que la date, l'heure et l'endroit. Les caméras fonctionnent 24 heures sur 24, 7 jours sur 7. La qualité des images, en fonction de la localisation, peut permettre l'identification de personnes. La majorité des caméras sont fixes. Quelques caméras sont dotées d'un zoom optique de puissance limitée permettant de zoomer sur un endroit ou une personne pour la suivre en cas de nécessité.

Le système de vidéosurveillance n'utilise pas de technologies dites intelligentes, n'est pas connecté à d'autres systèmes, n'utilise pas de surveillance dissimulée, n'effectue pas d'enregistrements de signaux sonores et n'utilise pas de "caméras de surveillance parlantes".

4.2 Objectif de la surveillance

L'Institution utilise son système de vidéosurveillance exclusivement à des fins de contrôle des accès et de sécurité (sécurité des personnes, des bâtiments et des informations).
Ces installations sont complémentaires aux systèmes de contrôle d'accès, aux systèmes de gestion des issues de secours et aux systèmes de sécurité incendie.
Le système de vidéosurveillance fait partie de l'ensemble des mesures mises en place pour soutenir la politique générale de sécurité et aide à prévenir, dissuader et, si nécessaire, à enquêter sur d'éventuels accès illégitimes (locaux à risques, infrastructures informatiques et informations opérationnelles).
En plus de cela, la vidéosurveillance aide à prévenir, détecter et enquêter sur les vols d'équipements ou de biens appartenant à l'Institution, à son personnel ou à des visiteurs. La vidéosurveillance contribue également à assurer la sécurité des usagers des bâtiments (par exemple en cas d'incendie, d'agression, etc.).

4.3 Limitation de l'objet

La vidéosurveillance est utilisée uniquement aux fins exposées ci-dessus. Le système de vidéosurveillance n'est pas utilisé pour évaluer le travail du personnel ou pour contrôler leur présence.
Le système n'est utilisé comme moyen d'enquête qu'en cas d'incident de sécurité (vols, intrusions non autorisées, etc.) et exceptionnellement, les images peuvent être transférées à d'autres instances officielles dans le cadre de l'exercice de leurs pouvoirs et compétences (enquêtes judiciaires, disciplinaires, OLAF, etc.). Ces transferts sont décrits dans le chapitre *6.5 Transferts et divulgation* ci-après.

4.4 Surveillance dissimulée

Aucune opération de surveillance dissimulée n'est prévue dans le cadre du système de vidéosurveillance. Toutefois, dans de rares cas et sans qu'il y ait de connexion avec le système de vidéosurveillance générale, l'institution peut avoir recours à des équipements de vidéosurveillance dissimulés.

L'utilisation de ces équipements ne pourra se faire qu'aux conditions suivantes :

- pour rechercher des auteurs d'intrusions répétées, de vols ou d'autres infractions graves aux règles de sécurité,
- pour une durée strictement limitée,
- dans des endroits bien précis,
- sur base d'une analyse d'impact soumise pour avis au Délégué à la Protection des données de l'Institution,
- et sur décision du Greffier de la Cour de justice de l'Union européenne.

Le délai d'emploi des équipements de vidéosurveillance dissimulée ne pourra dépasser la période d'occurrence des infractions ayant initiées leur emploi. Les équipements seront par ailleurs retirés dès identification du ou des auteur(s) des faits.

Les emplacements des équipements de vidéosurveillance dissimulée seront définis en fonction du lieu des infractions ayant initiées leur emploi. Ils ne pourront être placés dans des locaux où l'intimité est naturellement attendue (sanitaires).

La mise en place de caméras dissimulées répond à des conditions strictes, notifiées au CEPD aux fins d'un contrôle préalable, qui garantissent une incidence minimale sur la protection de la vie privée.

4.5 Webcams

Aucune webcam n'est reliée au système de vidéosurveillance de la Cour de justice de l'Union européenne.

4.6 Collecte de catégories spéciales de données

Aucune donnée, relevant des catégories spéciales de données visées à l'article 10 du règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des données à caractère personnel[3] n'est collectée.

Si des manifestations avaient lieu devant les bâtiments de la Cour de justice de l'Union européenne les garanties supplémentaires suivantes ont été prévues :

- La surveillance des manifestations n'est réalisée que pour des raisons sécuritaires ;
- Les caméras ne peuvent pas s'arrêter sur les visages de personnes et ne doivent pas essayer d'identifier des personnes, sauf en cas de menace imminente pour la sécurité publique ou de comportements criminels violents (vandalisme, agressions) ;
- Les images ne peuvent pas servir à des fins d'exploration de données[3] ;
- Tous les opérateurs qui exploitent les installations vidéo reçoivent une formation (voir ci-dessous point *6.3 Formation à la protection des données*) pour éviter tout impact disproportionné sur le respect de la vie privée et d'autres droits fondamentaux des participants filmés, y compris de leur liberté d'association.

5. Légitimation et base juridique du système de vidéosurveillance

L'utilisation du système de vidéosurveillance à des fins de sécurité et de contrôle des accès est nécessaire pour assurer le bon fonctionnement de l'Institution et l'exercice légitime de l'autorité publique dont elle est investie.

L'exploitation du système de vidéosurveillance, telle qu'elle est pratiquée par la Cour de justice de l'Union européenne, est conforme à l'article 5, sous a), du règlement nº 45/2001.

La présente politique de vidéosurveillance, qui s'inscrit dans un ensemble plus large de politiques de sécurité adoptées par l'Institution, fournit une base juridique plus détaillée et spécifique pour la vidéosurveillance.

6. Accès aux informations et données collectées

6.1 Section sécurité et sûreté de l'Institution et société de gardiennage

Des agents de sécurité d'une société de gardiennage sont chargés de visionner les images transmises en temps réel[4].
Les agents de sécurité de la société de gardiennage n'ont aucune possibilité d'accéder aux images enregistrées.

[3] Données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que des données relatives à la santé ou à la vie sexuelle.

[4] Cette société de gardiennage est un sous-traitant au sens de l'article 2, sous e), du règlement n° 45/2001. Ce sous-traitant traite les données personnelles dans les conditions prévues par l'article 23 du règlement n° 45/2001.

Le cahier des charges annexé au contrat de prestation de services conclu avec la société de gardiennage contient une clause de confidentialité ainsi qu'un article sur la protection des données pour garantir que les agents de sécurité respectent la protection des informations à caractère personnel. Ledit cahier des charges comporte également une référence spécifique à la vidéosurveillance (voir annexes 1a et 1b).

Les images enregistrées ne sont accessibles qu'au personnel de la Section sécurité et sûreté de l'Institution.
Tous les membres de la Section sécurité et sûreté sont tenus de signer une déclaration de confidentialité relative à l'utilisation du système de vidéosurveillance.

6.2 Droits d'accès

La « Procédure interne de vidéosurveillance »[5] indique clairement qui a accès aux images enregistrées et aux installations techniques du système de vidéosurveillance, sous quelles conditions et avec quels droits d'accès.

Un logiciel spécifique, un profil utilisateur et un mot de passe sont nécessaires pour avoir accès aux images enregistrées. Ce logiciel spécifique n'est installé que sur les ordinateurs de certains membres de la Section sécurité et sûreté de l'Institution.

6.3 Formation à la protection des données

Tout le personnel ayant des droits d'accès, y compris les agents de sécurité de la société de gardiennage, a reçu une formation relative à la protection des données.
Les nouveaux membres du personnel de sécurité reçoivent systématiquement une formation à leur arrivée dans le service.
Des ateliers consacrés au respect des règles de protection des données sont organisés tous les deux ans à l'intention du personnel ayant des droits d'accès.

6.4 Engagement de confidentialité du personnel de sécurité

Chaque membre de la Section sécurité et sûreté de l'Institution qui a le droit de traiter les images a signé une déclaration de confidentialité à l'issue de sa formation relative à la protection des données.
Chaque agent de la société de gardiennage qui a le droit de traiter les images a signé une déclaration de confidentialité à l'issue de sa formation relative à la protection des données.

[5] La Procédure interne de vidéosurveillance est un document interne, lequel précise qui est autorisé à visionner les images en temps réel, à visionner les images enregistrées, à copier les images, à exécuter un téléchargement, à effacer et à traiter images enregistrées.

6.5 Transferts et divulgation

Tout transfert ou divulgation de données ne peut être effectué que par le responsable du traitement des données, à savoir le Chef de la Section sécurité et sûreté, après consultation du DPD.
Tout acte de transfert ou de divulgation de données à des destinataires extérieurs à la Section sécurité et sûreté fait l'objet d'une évaluation rigoureuse quant à sa nécessité et à la compatibilité de ses finalités avec celles initialement poursuivies, à savoir la sécurité et le contrôle d'accès.

Ces transferts sont systématiquement consignés dans le registre de conservation et des transferts tenu par le Chef de la Section sécurité et sûreté.

La Direction des ressources humaines et de l'administration du personnel ne dispose d'aucun droit d'accès aux données traitées.

Dans les conditions définies par l'article 8 du règlement n° 45/2001, les images peuvent être transmises à la police luxembourgeoise si cela s'avère nécessaire aux fins d'une enquête menée dans l'exercice de ses compétences. En cas de doute, la Section sécurité et sûreté consulte le conseiller juridique pour les affaires administratives.

Les images peuvent aussi être transmises dans des circonstances exceptionnelles à :

- La Cour de justice (Cour), le Tribunal et/ou le Tribunal de la fonction publique (TFP) ou un juge national, ainsi que les avocats et agents des parties dans l'hypothèse d'un litige ;
- L'instance de la Cour, du Tribunal ou du TFP chargée d'examiner les réclamations, le Président et le Greffier de la juridiction concernée, ainsi que le conseiller juridique pour les affaires administratives, en cas de réclamation introduite en application de l'article 90, paragraphe 2, du statut des fonctionnaires ;
- L'OLAF en cas d'enquête effectuée en application du règlement n° 883/2013 et de la décision de la Cour de justice du 12 juillet 2011 relative aux conditions et modalités des enquêtes internes en matière de lutte contre la fraude, la corruption et toute activité illégale préjudiciable aux intérêts de l'Union européenne ;
- Les personnes appelées à exercer des fonctions dans le cadre d'une enquête administrative ordonnée par l'autorité investie du pouvoir de nomination ou l'autorité habilitée à conclure les contrats d'engagements ou dans le cadre d'une procédure disciplinaire, ouverte, selon les règles définies à l'annexe IX du statut des fonctionnaires de l'UE, à la suite d'un incident de sécurité ;
- Le Président et le Greffier de la Cour, ainsi que des fonctionnaires qui les assistent, dans le cadre des responsabilités qui leur sont dévolues par l'article 20, paragraphe 4, du règlement de procédure de la Cour ;
- Le CEPD conformément à l'article 47, paragraphe 2, du règlement n° 45/2001 ;
- Le DPD de l'Institution conformément au point 4 de l'annexe au règlement n° 45/2001 ;
- Le Médiateur européen dans la mesure nécessaire au traitement d'une plainte auprès de lui (article 228 TFUE).

7. Mesures de protection des données et informations

Les principales mesures techniques et organisationnelles mises en place pour protéger la sécurité du système de vidéosurveillance, y compris les données à caractère personnel, sont les suivantes :

- Les serveurs sur lesquels les images sont enregistrées se trouvent dans des locaux sécurisés, protégés par des mesures de sécurité physique ; des firewalls sont installés pour protéger les installations IT ;
- Chaque membre du personnel de sécurité (interne et externe) a signé une déclaration de confidentialité ;
- Les droits d'accès des utilisateurs au système de vidéosurveillance sont limités aux outils nécessaires pour exécuter leur travail ;
- Seul le gestionnaire du système, désigné par le responsable du traitement, est habilité à attribuer, modifier ou annuler les droits d'accès des utilisateurs. L'attribution, la modification ou la suppression des droits d'accès se fait conformément aux critères définis dans la Procédure interne de vidéosurveillance ;
- La Procédure interne de vidéosurveillance contient une liste à jour des personnes qui ont accès au système, dans laquelle la portée de leurs droits d'accès est précisée.

8. Conservation des données

Les images sont conservées pour une durée de 30 jours au maximum.
Au-delà de 30 jours, les enregistrements sont automatiquement écrasés.
Ce délai se justifie par :

- L'expérience actuelle selon laquelle des incidents de sécurité sont souvent reportés à la Section sécurité et sûreté de l'Institution plus de deux semaines après les faits ;
- La pratique de malfaisants / terroristes qui consiste à effectuer un repérage des bâtiments avant de commettre un acte illicite ;
- Le nombre élevé de visiteurs qui est d'environ 100 000 personnes par an.

Certaines images peuvent être conservées pendant une période plus longue si cette conservation est nécessaire aux fins d'une enquête ou pour servir comme preuve relative à un incident de sécurité. Cette conservation est documentée (registre électronique) et les raisons pour lesquelles les images sont conservées pour une durée excédant 30 jours sont précisées. Une copie papier du registre de conservation et des transferts se trouve en annexes 2a et 2b. La nécessité de cette conservation est réévaluée régulièrement.

La vidéosurveillance est suivie en temps réel par les agents de sécurité dans le poste de commandement sûreté et incendie (PCS/PCI), et ce, 24 heures sur 24, 7 jours sur 7.

9. Information du public et information individuelle spécifique

9.1 Information via différents medias

Une information appropriée et exhaustive sur la vidéosurveillance est mise à la disposition du public. Cette information est donnée par les media suivants :

- Des panneaux d'avertissement sont placés aux différents accès des bâtiments. Ces panneaux signalent la présence d'un système de vidéosurveillance et précisent notamment la durée de conservation des images ainsi que les coordonnées pour prendre contact avec le service responsable ;
- Une notice informative comportant les informations prescrites par l'article 12 du règlement n° 45/2001 est disponible aux réceptions des bâtiments, sur les sites intranet de la Section sécurité et sûreté et du délégué à la protection des données ainsi que sur le site web de l'Institution (http://curia.europa.eu/jcms/jcms/P_127468 : L'institution > Se rendre à la Cour > Conditions générales). Cette notice comporte un numéro de téléphone ainsi qu'une adresse e-mail afin de permettre aux personnes intéressées d'obtenir des renseignements complémentaires ;
- La présente politique de vidéosurveillance est accessible sur les sites intranet de la Section sécurité et sûreté et du délégué à la protection des données ainsi que sur le site internet de la Cour de justice de l'Union européenne (cf. point 2.6 Transparence).

Des copies des panneaux d'avertissement et de la notice informative sont jointes en annexes 3a et 3b.

9.2 Notification individuelle spécifique

Quand des personnes sont identifiées sur les images (par exemple pour une enquête de sécurité), elles doivent en être informées à titre individuel si au moins une des conditions suivantes est remplie :

- Leur identité est notée dans un fichier ;
- La séquence vidéo est utilisée contre la personne en question ;
- La séquence vidéo est conservée pour une durée plus longue que la période prévue ;
- La séquence vidéo est transférée en dehors de la Section sécurité et sûreté ;
- L'identité de la personne est communiquée à des personnes en dehors de la Section sécurité et sûreté.

Cette information individuelle peut être retardée, conformément à l'article 20, paragraphe 1, sous a), du règlement n° 45/2001 si cela est nécessaire pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales. Le DPD est consulté dans le cas où l'application de cette limitation est envisagée.

10. Droits des personnes concernées

Les personnes filmées ont le droit d'accéder aux données personnelles les concernant et de faire rectifier ces données si elles sont inexactes ou incomplètes.

Pour ce qui est de l'exercice du droit d'accès, il est possible d'organiser un visionnage des images ou de fournir au demandeur une copie des images enregistrées. Dans ce cas, le demandeur doit présenter une pièce d'identité avant le visionnage des images. Il doit aussi indiquer la date, l'heure, l'endroit et les circonstances dans lesquelles il a été enregistré.

Actuellement, les demandeurs peuvent visionner gratuitement les images, et, si la personne concernée a un intérêt légitime à faire valoir, obtenir une copie sans frais. Le principe de la gratuité pourrait être revu dans le cas où le nombre de demandes augmenterait d'une manière significative.

Dans les conditions prévues par les articles 15 et 16 du règlement n° 45/2001, les personnes concernées peuvent aussi obtenir le verrouillage ou l'effacement des données personnelles qui les concernent. En cas de demande d'effacement, le responsable du traitement consulte le DPD.

Les droits des personnes concernées peuvent faire l'objet d'une limitation conformément à l'article 20, paragraphe 1, sous a), du règlement n° 45/2001 si cela est nécessaire pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales.

Les droits des personnes concernées peuvent aussi faire l'objet d'une limitation au titre de l'article 20, paragraphe 1, sous c), du règlement n° 45/2001, si cela s'avère nécessaire pour garantir la protection de la personne concernée ou des droits et libertés d'autrui.
Par exemple, si une personne concernée souhaite accéder aux séquences sur lesquelles elle apparaît, il pourrait être nécessaire de limiter son droit d'accès au cas où une autre personne apparaitrait également dans les mêmes séquences et que le consentement de cette dernière ne serait pas obtenu, dans la mesure où le système de vidéosurveillance actuellement utilisé ne permet pas de masquer l'image d'une personne.

Le responsable du traitement consulte le DPD dans le cas où l'application d'une limitation aux droits des personnes concernées est envisagée.

Toute demande d'accès, de rectification, de verrouillage, ou d'effacement doit être adressée au :

Chef de la Section Sécurité et Sûreté, Responsable du traitement des données
Cour de justice de l'Union européenne
L-2925 Luxembourg
tel : +352 4303-1
securite@curia.europa.eu

La Section sécurité et sûreté peut aussi être contactée pour toute autre question relative au traitement des données à caractère personnel concernant le système de vidéosurveillance mis en place à la Cour.

Si possible, la Section sécurité et sûreté répondra endéans les 15 jours ouvrables à toute demande. S'il n'est pas possible de respecter ce délai, le demandeur sera informé endéans les 15 jours de la suite de sa demande ainsi que des raisons pour lesquelles sa demande n'a pu être traitée dans le délai prévu. Dans tous les cas une réponse doit être fournie au plus tard dans les 3 mois.

11. Droit de recours

Au titre de l'article 32, paragraphe 2, du règlement n° 45/2001, sans préjudice d'un recours juridictionnel, toute personne concernée peut présenter une réclamation au CEPD (edps@edps.europa.eu) si elle estime que les droits qui lui sont reconnus à l'article 16 du traité sur le fonctionnement de l'Union européenne ont été violés à la suite d'un traitement de données à caractère personnel effectué par l'Institution.

Avant de présenter une telle réclamation, les personnes concernées sont invitées à essayer d'obtenir satisfaction en contactant :

le **Chef de la Section sécurité et sûreté, Responsable du traitement des données**
Cour de justice de l'Union européenne
L-2925 Luxembourg
tel. : +352 4303-1
securite@curia.europa.eu

et/ou

le **Délégué à la Protection des Données**
Cour de justice de l'Union européenne
L-2925 Luxembourg
tel : +352 4303-1
DataProtectionOfficer@curia.europa.eu

Les membres du personnel, conformément à l'article 90 du statut des fonctionnaires, peuvent demander un examen auprès de l'autorité investie de pouvoir de nomination / autorité habilitée à conclure les contrats d'engagement.

Annexes

Annexe 1a *Extrait de l'article 16 du contrat CJ 03/2010 portant sur la protection des données*

Annexe 1b: *Extrait du cahier des charges de l'appel d'offres CJ 03/2010 portant sur le système de vidéosurveillance*

Annexe 2a : *Registre de conservation des données*

Annexe 2b : *Registre des transferts des données*

Annexe 3a: *Panneaux d'avertissement*

Annexe 3b: *Notice informative*

Annexe 1a à la Politique de vidéosurveillance

Article 16 - Protection des données

1. Données traitées par la Cour de justice de l'Union européenne

   a. La Cour de justice de l'Union européenne traite les données à caractère personnel conformément au règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

   b. Ces données seront traitées exclusivement aux fins de l'exécution, de la gestion et du suivi du contrat par l'Unité « Affaires immobilières et Sécurité » et la division budget et comptabilité, sans préjudice d'une éventuelle transmission de ces données aux organes chargés d'une mission de contrôle ou d'inspection conformément au droit de l'Union européenne.

   c. Dans l'hypothèse où le contractant se trouverait dans l'une des situations d'exclusion visées par les articles 93 et 94 du règlement financier règlement nº 1605/2002 du Conseil du 25 juin 2002), des données le concernant sont enregistrées dans la base de données prévue par l'article 95 du même règlement et susceptibles d'être communiquées par la Commission aux personnes habilitées à les recevoir, désignées par les autres institutions, agences, autorités ou organismes visés à cet article en application de l'article 134 bis, paragraphe 2, du règlement nº2342/2002 portant modalités d'exécution du règlement financier, tel que modifié et du règlement (CE,17 / 109 COUR DE JUSTICE DE L'UNION EUROPEENNE Appel d'offres CJ 03/2010 26 mars 2010 Euratom) nº 1302/2008 de la Commission du 17 décembre 2008 relatif à la base de données centrale sur les exclusions.

   d. Dans le cadre de l'exécution d'un contrat, les catégories de données suivantes peuvent ainsi être traitées : nom, adresse, numéro de téléphone et de télécopieur, adresse de courrier électronique ;

   ➔ Données contenues dans le passeport ou le certificat de nationalité (copie)
   ➔ Preuve du statut d'indépendant, preuve du statut fiscal ;
   ➔ Données bancaires (numéro de compte, nom de la banque, code IBAN);
   ➔ Données contenues dans un extrait de casier judiciaire, un certificat attestant le (non) paiement des cotisations de sécurité sociale ou d'impôts
   ➔ Curriculum vitae ;
   ➔ Liste des principales publications ou réalisations ;
   ➔ Déclaration mentionnant le chiffre d'affaires du soumissionnaire;
   ➔ Déclaration des banques ou preuve d'une assurance des risques professionnels ;
   ➔ Autres données en rapport avec le contractant, transmises par ce dernier dans le cadre de l'exécution du contrat.

Par ailleurs, des données à caractère personnel sont générées par les personnes participant à l'évaluation de l'exécution du contrat (en particulier des données d'évaluation).

e. La Cour des Comptes, le comité spécialisé en matière d'irrégularités financières, l'auditeur interne (dans le cadre des fonctions qui lui sont dévolues par les articles 85 à 87 du règlement financier), le Parlement européen (dans le cadre de la procédure de décharge), l'OLAF, le comité de surveillance de l'OLAF (en application de l'article 11 du règlement nº 1073/1999), le Tribunal de l'Union européenne et la Cour de justice de l'Union européenne, les tribunaux compétents (généralement les tribunaux luxembourgeois) en cas de litige portant sur l'exécution du marché, le Président et le Greffier de la Cour de justice de l'Union européenne ainsi que les fonctionnaires qui les assistent dans le cadre des responsabilités qui leur sont dévolues par l'article 23 du règlement de procédure de la Cour de justice de l'Union européenne et le conseiller juridique pour les affaires administratives, peuvent être destinataires dans le cadre de leurs attributions respectives.

f. En vertu de l'article 49 du règlement nº 2342/2002, les documents relatifs au marché et contenant les données à caractère personnel sont conservés pendant cinq ans à partir de la décharge du Parlement afférente au budget de l'année au cours de laquelle a lieu le dernier acte d'exécution du marché ou au cours de laquelle expire la garantie conventionnelle ou légale dont bénéficie le pouvoir adjudicateur dans le cadre du marché. Les données à caractère personnel contenues dans les pièces justificatives sont supprimées si possible lorsqu'elles ne sont pas nécessaires aux fins de la décharge budgétaire, du contrôle et de l'audit.

g. Le contractant, ainsi que les personnes concernées par des données à caractère personnel traitées dans le cadre de l'exécution du présent contrat, peuvent, sur demande, obtenir la communication de leurs données à caractère personnel et la 18 / 109 COUR DE JUSTICE DE L'UNION EUROPEENNE Appel d'offres CJ 03/2010 26 mars 2010 rectification de données inexactes ou incomplètes. Pour toute question au sujet du traitement de ces données, elles sont priées de s'adresser au chef de l'Unité « Affaires immobilières et sécurité ». Elles ont également le droit de saisir à tout moment le Contrôleur européen de la protection des données.

h. Le(s) représentant(s) du contractant est (sont) tenu(s) d'informer les personnes auxquelles se rapportent des données à caractère personnel utilisées dans le cadre du présent contrat, de la nature, des finalités et des caractéristiques du traitement (catégories de données, de destinataires, délai de conservation, etc.) ainsi que des droits décrits ci-dessus.

2. <u>Données traitées pour le compte de la Cour de justice de l'Union européenne</u>

   a. Le contractant agit sur instruction du responsable du traitement.

b. Il se conforme aux règles applicables relatives à la protection des données à caractère personnel.

c. En ce qui concerne la confidentialité et la sécurité des données, les obligations visées aux articles 21 et 22 du règlement (CE) n° 45/2001 incombent également au contractant, à moins que, en vertu de l'article 16 ou de l'article 17, paragraphe 3, deuxième tiret, de la directive 95/46/CE, le contractant soit déjà soumis à des obligations de confidentialité et de sécurité énoncées dans la législation nationale de l'un des États membres.

7.2.3. Système de contrôle d'accès et de détection anti-intrusion

La Cour de justice mettra à la disposition du Prestataire un système centralisé déployé sur l'ensemble du site permettant le contrôle des accès et la détection d'intrusion. Son exploitation en temps réel sera réalisée à travers l'outil de GSC. Toutefois, en mode dégradé, l'agent en poste au PCS sera en mesure d'exploiter le sous-système natif.
Le module de gestion des visiteurs est, quant à lui, exploité par les agents et hôtesses aux postes d'accueil.

7.2.4. Système de vidéosurveillance

7.2.4.1. Général

La Cour de justice mettra à la disposition du Prestataire, le système central entièrement numérique, constitué des équipements et sous-systèmes suivants :

➔ Caméras de vidéosurveillance fixes et mobiles ;

➔ Enregistreurs numériques à haute capacité de stockage assurant la fonction de matriçage et d'enregistrement automatique continu de pré et post alarme et d'enregistrement d'images fixes ;

➔ Système de vidéo détection intérieure et extérieure (détection automatique de mouvement dans le champ d'une caméra).

La surveillance des principaux obstacles de contrôle d'accès et des zones sensibles est assurée par des caméras fixes.

La surveillance extérieure aux abords des bâtiments est assurée par des caméras fixes avec vidéo détection, complétée par des caméras mobiles pour assurer la levée de doute.

L'exploitation en temps réel du système de vidéosurveillance sera réalisée à travers l'outil de GSC. Toutefois, en mode dégradé, l'agent en poste au PCS sera en mesure d'exploiter le sous-système natif.

7.2.4.2. Respect de la vie privée – protection des données

Le Prestataire agit sur instruction du responsable du traitement. Il se conforme aux règles Applicables relatives à la protection des données à caractère personnel, et notamment :

➔ Au règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et plus particulièrement aux dispositions relatives à la confidentialité et la sécurité des données (articles 21 et 22 du règlement);

➔ Aux lignes directrices relatives à la vidéosurveillance du Contrôleur européen de la protection des données (CEPD);

➔ A la politique de vidéosurveillance de la Cour de justice;

➔ Aux consignes données par la Cour de justice ;

➔ Aux recommandations du Contrôleur européen de la protection des données (CEPD) ou du Délégué à la protection des données de la Cour de justice dans le cadre de l'exercice de leurs fonctions de contrôle/inspection ou consultation.
Le Prestataire s'engage à donner une formation adaptée au personnel qui exploite les caméras, portant notamment sur les obligations en matière de protection des données et les lignes directrices relatives à la vidéosurveillance du Contrôleur européen de la protection des données (CEPD).

Annexe 2a - Registre de conservation des données

REGISTRE DE CONSERVATION DES ENREGISTREMENTS (selon article 7.2 des lignes directrices)									
N°	Date incident	Heure		Caméra		Description incident	Raison conservation	Date estimée de reévaluation	Nom de l'enregistrement
		début	fin	Numéro	Position				
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									
25									
26									
27									
28									
29									
30									
31									
32									
33									
34									
35									
36									
37									
38									
39									
40									
41									
42									
43									
44									
45									
46									
47									
48									
49									
50									

Annexe 2b - Registre de transfert des données

REGISTRE DES TRANSFERTS ET DIVULGATIONS DES ENREGISTREMENTS (selon article 10.5 des lignes directrices)														
N°	Date incident	Identification de la personne requérante				Personne ayant autorisé le transfert			Description succinte du contenu des enregistrements	Motivation de la demande et de l'autorisation de transmission	Transmission	Montré	Si informations orales transmises, préciser la nature
		Nom	Prénom	Fonction	Service	Nom	Prénom	Fonction					
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													
21													
22													
23													
24													
25													
26													
27													
28													
29													
30													
31													
32													
33													
34													
35													
36													
37													
38													
39													
40													
41													
42													
43													
44													
45													
46													
47													
48													
49													
50													

Annexe 3a - Panneaux avertissement

VIDÉOSURVEILLANCE

Pour votre sécurité, ce bâtiment et son voisinage immédiat sont placés sous vidéosurveillance.

Les images sont conservées pendant 30 jours.

Pour de plus amples informations, veuillez consulter la page http://curia.europa.eu/jcms/jcms/P_127468 ou prendre contact avec la section sécurité en téléphonant au +352 43031ou en adressant un courriel à securite@curia.europa.eu

VIDEOÜBERWACHUNG

Zu Ihrer Sicherheit werden dieses Gebäude und seine unmittelbare Umgebung videoüberwacht.

Die Aufnahmen werden 30 Tage lang gespeichert.

Weitere Auskünfte erhalten Sie unter der adresse http://curia.europa.eu/jcms/jcms/P_127468 Sie Können sich aber auch mit der Sicherheitsabteilung unter +352 43031 oder securite@curia.europa.eu in Verbindung setzen

VIDEO SURVEILLANCE

For your safety and security, this building and its immediate vicinty are under video-surveillance.

Recording are retained for 30 days.

For further information, please consult http://curia.europa.eu/jcms/jcms/P_127468 or contact the security section at +352 43031 or securite@curia.europa.eu

Annexe 3b – Notice informative

Notice informative relative à la vidéosurveillance dans les bâtiments de la Cour de justice de l'Union européenne

La présente notice fournit des informations relatives au système de vidéosurveillance générale mis en place par l'institution (1) ainsi que des informations concernant la possibilité de recourir à un dispositif ad hoc (2).

1) Informations relatives à la vidéosurveillance générale

L'institution a mis en place un système de vidéosurveillance pour assurer la sécurité générale des personnes et des biens conformément au Schéma directeur de mise en sûreté du complexe immobilier de la Cour de justice de l'Union européenne. Les finalités et les modalités du traitement des images filmées sont détaillées dans un document intitulé « Politique de vidéosurveillance » accessible sur le site internet de l'institution ainsi que sur les sites intranet de la Section sécurité et sûreté et du délégué à la protection des données.

Des caméras de surveillance sont placées tant à l'extérieur qu'à l'intérieur des bâtiments de l'institution (sélection aléatoire ou commandée des lieux filmés).

Les images des personnes concernées (personne accédant aux bâtiments de l'institution ou se trouvant aux abords extérieurs desdits bâtiments) sont les seules données collectées par le système.

La personne responsable du traitement des données est le Chef du Service de sécurité, tel +352 4303-1, securite@curia.europa.eu.

Les images sont enregistrées et utilisées conformément :

- au règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données,
- aux recommandations du Contrôleur européen de la protection des données (« CEPD ») reprises dans les lignes directrices en matière de vidéo surveillance du 17 mars 2010[1].

[1] Les lignes directrices en matière de vidéosurveillance sont disponibles sur le site internet du CEPD : https://secure.edps.europa.eu/EDPSWEB/edps/lang/fr/Supervision/Guidelines

Les images sont traitées pour les finalités suivantes :

- Contrôles d’accès et de sécurité (sécurité des personnes, des bâtiments, des biens et des informations) ;
- Localisation d’un départ de feu, estimation d'impact pour une éventuelle évacuation d’un bâtiment, surveillance des issues de secours ;
- Surveillance des œuvres d'art ;
- Dissuasion (dégradations des biens de l'institution, atteintes aux personnes) ;
- Recherche des auteurs d'éventuelles infractions.

Les images enregistrées sont conservées pendant une durée maximale de 30 jours, mais, en cas de suspicion et/ou de constatation d’infraction, les données pertinentes sont conservées pendant la durée de l’enquête et de la procédure (par ex. disciplinaire ou pénale) qui éventuellement en découle. Les images enregistrées ne sont accessibles qu'à un nombre limité de personnes et toutes les mesures techniques et physiques sont mises en œuvre afin d'en éviter une utilisation inadéquate.

Les personnes suivantes ont accès aux images :

- Fonctionnaires et agents du Service de sécurité de la Direction des bâtiments (visualisation, enregistrement, copie, archivage, effacement) ;
- Agents de la société de gardiennage qui assurent partiellement les fonctions de sécurité (visualisation en temps réel sans accès aux images enregistrées).

Les images peuvent être communiquées à d'autres destinataires dans des cas particuliers :

- la Cour de justice (« Cour »), le Tribunal de l’Union européenne (« Tribunal ») et/ou le Tribunal de la fonction publique (« TFP »), ou un juge national, ainsi que les avocats et agents des parties dans l'hypothèse d'un litige ;
- l’instance de la Cour, du Tribunal, ou du TFP chargée d'examiner les réclamations, le Président et le Greffier de la juridiction concernée, ainsi que le conseiller juridique pour les affaires administratives, en cas de réclamation introduite en application de l'article 90, paragraphe 2, du statut des fonctionnaires ;
- les personnes appelées à exercer des fonctions dans le cadre d’une enquête administrative ordonnée par l’autorité investie du pouvoir de nomination ou l’autorité habilitée à conclure les contrats d’engagements ou dans le cadre d’une procédure disciplinaire, ouverte, selon les règles définies à l’annexe IX du statut des fonctionnaires de l’UE, à la suite d’un incident de sécurité ;
- le Président et le Greffier de la Cour, ainsi que des fonctionnaires qui les assistent, dans le cadre des responsabilités qui leur sont dévolues par l'article 20, paragraphe 4, du règlement de procédure de la Cour ;
- le CEPD conformément à l'article 47, paragraphe 2, du règlement n° 45/2001 ;
- le délégué à la protection des données de l'institution conformément au point 4 de l'annexe au règlement n° 45/2001 ;
- le Médiateur européen dans la mesure nécessaire au traitement d'une plainte auprès de lui (article 228 TFUE) ;
- l’OLAF en cas d'enquête effectuée en application du règlement n° 883/2013 et de la décision de la Cour de justice du 12 juillet 2011 relative aux conditions et modalités des

enquêtes internes en matière de lutte contre la fraude, la corruption et toute activité illégale préjudiciable aux intérêts de l'Union européenne.

Enfin, dans les conditions définies par l'article 8 du règlement n° 45/2001, les images peuvent être transmises aux autorités nationales si cela s'avère nécessaire aux fins d'une enquête menée dans l'exercice de ses compétences.

Tous les transferts de données effectués sont consignés dans un registre spécifique.

Toute personne qui souhaite obtenir des informations supplémentaires ou exercer les droits qu'elle tire du règlement n° 45/2001 (accès, rectification, verrouillage, effacement ou opposition) peut s'adresser au Chef du Service de sécurité.

Les articles 13 et 14 du règlement n° 45/2001, relatifs, respectivement, au droit d'accès et au droit de rectification, sont cités *in extenso* ci-après.

La personne dont les données personnelles sont traitées a aussi la possibilité de saisir le CEPD au titre de l'article 32, paragraphe 2, du règlement n° 45/2001.

Article 13 du règlement n° 45/2001

Droit d'accès

La personne concernée a le droit d'obtenir, sans contrainte, à tout moment dans un délai de trois mois à partir de la réception de la demande d'information et gratuitement, du responsable du traitement :
a) la confirmation que des données la concernant sont ou ne sont pas traitées;
b) des informations au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées;
c) la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données;
d) la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant.

Article 14 du règlement n° 45/2001

Rectification

La personne concernée a le droit d'obtenir du responsable du traitement la rectification sans délai de données à caractère personnel inexactes ou incomplètes.

2) Informations relatives à la vidéosurveillance dissimulée (chapitre 4.4 de la politique de vidéosurveillance de la Cour de justice de l'Union européenne, « vidéosurveillance dissimulée »)

Le système de vidéosurveillance générale ne comprend aucun dispositif de vidéosurveillance dissimulée.

Dans le cadre d'une investigation interne de sécurité, sur base d'une analyse d'impact (soumise pour avis au délégué à la protection des données) et après décision du Greffier de la Cour, l'institution peut à titre exceptionnel avoir recours à un système de vidéosurveillance dissimulée, distinct et déconnecté du système de vidéosurveillance générale, pour rechercher des auteurs d'intrusions répétées, de vols ou d'autres infractions graves aux règles de sécurité.

L'analyse d'impact doit permettre de démontrer en quoi l'atteinte à la vie privée et à la protection des données à caractère personnel résultant de l'utilisation d'un système de vidéosurveillance dissimulée est compensée par les avantages tirés de l'utilisation dudit système.
À cette fin, cette analyse prend en compte, en sus des garanties qui encadrent l'utilisation de la vidéosurveillance générale, un ensemble de critères, parmi lesquels figurent l'absence de mesures alternatives plus respectueuses de la vie privée ainsi que les limites appliquées à l'emploi des équipements envisagés (lieu, horaires et délai de recours aux équipements, dont le choix est lui-même déterminé en fonction des infractions constatées).

Les équipements de vidéosurveillance dissimulée ne peuvent en aucun cas être connectés au système de vidéosurveillance générale. De ce fait, les images enregistrées sont relevées manuellement.
Ces images sont visionnées dès que possible et au plus tard endéans sept jours ouvrables suivant leur enregistrement afin d'en évaluer la pertinence. Cette durée maximale de sept jours ouvrables est nécessaire dans la mesure où des interventions quotidiennes sur les équipements pourraient nuire au bon déroulement de l'investigation interne de sécurité, mais aussi afin de disposer de suffisamment de temps pour procéder au relevé manuel des images sur lesdits équipements.

Les images qui ne sont pas pertinentes aux fins de l'investigation interne de sécurité sont effacées immédiatement après leur premier visionnage.
Les images pertinentes aux fins de l'investigation interne de sécurité sont conservées jusqu'à la clôture de cette investigation et des procédures faisant éventuellement suite à celle-ci.

Les personnes identifiées sur les images sont informées à titre individuel par la Section sécurité et sûreté si au moins l'une des conditions suivantes est remplie :

- l'identité de la personne a été notée dans un dossier;
- l'enregistrement vidéo est utilisé à l'encontre de la personne;
- l'enregistrement vidéo est conservé au-delà des délais prévus ci-dessus;
- l'enregistrement vidéo est transféré à l'extérieur de la Section sécurité et sûreté ou
- l'identité de la personne est communiquée à une personne extérieure à la Section sécurité et sûreté.

Cette information peut être retardée si cela est nécessaire aux fins de l'investigation interne de sécurité ou dans d'autres cas prévus par l'article 20 du règlement n° 45/2001 (cité *in extenso* ci-après).

Article 20 du règlement n° 45/2001

Exceptions et limitations

1. Les institutions et organes communautaires peuvent limiter l'application de l'article 4, paragraphe 1, de l'article 11, de l'article 12, paragraphe 1, des articles 13 à 17 et de l'article 37, paragraphe 1, pour autant qu'une telle limitation constitue une mesure nécessaire pour:

a) assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales;

b) sauvegarder un intérêt économique ou financier important d'un État membre ou des Communautés européennes, y compris dans les domaines monétaire, budgétaire et fiscal;

c) garantir la protection de la personne concernée ou des droits et libertés d'autrui;

d) assurer la sûreté nationale, la sécurité publique et la défense des États membres;

e) assurer une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) et b).

2. Les articles 13 à 16 ne s'appliquent pas lorsque les données sont traitées exclusivement aux fins de la recherche scientifique ou sont stockées sous la forme de données à caractère personnel pendant une durée n'excédant pas celle qui est nécessaire à seule fin d'établir des statistiques, sous réserve qu'il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne concernée et que le responsable du traitement offre des garanties juridiques appropriées, qui excluent notamment que les données puissent être utilisées aux fins de mesures ou de décisions se rapportant à des personnes déterminées.

3. Si une limitation prévue au paragraphe 1 est imposée, la personne concernée est informée conformément au droit communautaire des principales raisons qui motivent cette limitation et de son droit de saisir le contrôleur européen de la protection des données.

4. Si une limitation prévue au paragraphe 1 est invoquée pour refuser l'accès à la personne concernée, le contrôleur européen de la protection des données lui fait uniquement savoir, lorsqu'il examine la réclamation, si les données ont été traitées correctement et, dans la négative, si toutes les corrections nécessaires ont été apportées.

5. L'information visée aux paragraphes 3 et 4 peut être reportée aussi longtemps qu'elle prive d'effet la limitation imposée sur la base du paragraphe 1.