Bruxelles, 17 mars 2010

LIGNES DIRECTRICES DU CEPD EN MATIÈRE DE VIDÉOSURVEILLANCE

Table des matières

Avant-propos

Les présentes lignes directrices contiennent un ensemble de recommandations destinées à guider les institutions et organes de l'Union européenne dans la conception et l'utilisation de leurs systèmes de vidéosurveillance. Les systèmes de vidéosurveillance bien conçus et utilisés à bon escient sont un outil puissant dans la lutte contre les problèmes de sécurité. Les systèmes mal conçus, par contre, engendrent un faux sentiment de sécurité tout en enfreignant notre vie privée et en restreignant nos autres droits fondamentaux.

La sécurité et le respect des droits fondamentaux ne doivent pas s'exclure mutuellement. Moyennant l'adoption d'une approche pragmatique basée sur les principes de la sélectivité et de la proportionnalité, les systèmes de vidéosurveillance peuvent répondre aux besoins de sécurité tout en respectant notre vie privée. Les caméras peuvent et doivent être utilisées de façon intelligente et ne viser que des problèmes de sécurité clairement identifiés, diminuant ainsi le plus possible la capture d'images inutiles. Cette approche permet non seulement de réduire le plus possible les atteintes à la vie privée, mais aussi d'utiliser la vidéosurveillance d'une façon plus ciblée et finalement plus efficace.

Dans les limites prévues par la législation sur la protection des données, chaque institution et organe européen dispose d'une marge d'appréciation sur la manière de concevoir son propre système. Dans le même temps, chaque institution doit également démontrer que des procédures sont en place afin d'assurer la conformité avec les exigences de protection des données. D'un point de vue organisationnel, les pratiques recommandées comprennent l'adoption d'une série de garanties en matière de protection des données devant être décrites dans la politique de vidéosurveillance de l'institution et des audits périodiques pour vérifier la conformité.

Dans certains cas présentant un risque particulièrement élevé d'atteinte aux droits fondamentaux (par exemple une surveillance dissimulée ou une surveillance préventive dynamique), une analyse d'impact en matière de respect de la vie privée et de protection des données devra également être réalisée et soumise au CEPD pour permettre un contrôle préalable. Hormis ces exceptions par contre, il n'est pas nécessaire d'impliquer étroitement le CEPD dans la prise de décision relative à la conception d'un système particulier.

La protection des données ne devrait pas être considérée comme un fardeau réglementaire ou une case de conformité devant être «cochée». Elle devrait au contraire faire partie de la culture organisationnelle et de la bonne gouvernance au sein desquelles les décisions sont prises par la direction de chaque institution sur la base des conseils de leurs délégués à la protection de données et des consultations avec les parties prenantes.

Nous espérons que nos lignes directrices vous seront utiles dans le cadre de vos efforts de conformité.

(signé)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données

1 Objectif des lignes directrices

Les présentes lignes directrices («**lignes directrices**») ont été émises par le contrôleur européen de la protection des données («**CEPD**») en exécution des pouvoirs qui lui sont conférés par l'article 47 du règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires[1] («**règlement**»).

Ces lignes directrices ont pour objectif d'offrir aux institutions et organes («**institutions**»)[2] de l'Union européenne (anciennement «Communauté européenne») qui utilisent un matériel de vidéosurveillance des conseils sur la manière de respecter le règlement et d'utiliser la vidéosurveillance de façon responsable tout en mettant en place des garanties efficaces. Elles énoncent les principes permettant d'évaluer la nécessité de recourir à la vidéosurveillance et fournissent des orientations sur la façon d'en minimiser l'impact sur la vie privée et autres droits fondamentaux.

Ces lignes directrices sont destinées aux personnes qui décident d'installer ou non des systèmes de vidéosurveillance et qui sont chargées de leur exploitation (les «**responsables du traitement**» au sens de la réglementation sur la protection des données[3]). Il s'agit généralement des services de sécurité des institutions, mais aussi de la haute hiérarchie des institutions assumant la responsabilité ultime des décisions. Ces lignes directrices ont également pour objectif de guider les fournisseurs ou autres contractants participant à l'installation et à l'exploitation (parfois en qualité de «**sous-traitants**»[4]) ainsi que les délégués à la protection des données («**DPD**»[5]), les membres du personnel et le grand public.

Ces lignes directrices ne constituent pas un exposé de points de droit. Elles présentent au contraire des recommandations et proposent des bonnes pratiques tout en admettant qu'il peut exister des exceptions à la règle et que, dans les limites prévues par la législation sur la protection des données, chaque institution dispose

---

[1] Règlement (CE) n° 45/2001 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, JO L 8, 12.01.2001, p. 1.

[2] Depuis l'entrée en vigueur du traité de Lisbonne, le paysage juridique de l'Union européenne a changé considérablement. L'un des changements les plus importants a été l'abolition de la structure en piliers, et donc l'inclusion des domaines de politiques du troisième pilier dans le domaine de l'ancien premier pilier. Ces changements ont également des conséquences pour le travail du CEPD et soulèvent des questions quant au champ d'application des règles existantes en matière de protection des données aux institutions et organes de l'Union. Sans préjudice de toute autre interprétation ou révision possible de l'article 3, paragraphe 1 du règlement, le CEPD propose déjà une assistance et des conseils à toutes les institutions selon les besoins et leur recommande de suivre les présentes lignes directrices.

[3] Voir l'article 2, point d) du règlement.

[4] Voir l'article 2, point e) du règlement.

[5] Voir l'article 24 du règlement.

d'un pouvoir d'appréciation quant à la façon de concevoir son propre système.Les lignes directrices se veulent souples: elles ont été conçues pour permettre une personnalisation. Cette flexibilité doit empêcher qu'une interprétation rigide ou bureaucratique des préoccupations de protection des données ne vienne entraver la satisfaction de besoins réels de sécurité ou la réalisation d'autres objectifs légitimes.

Ceci étant dit, la meilleure façon de respecter la législation est souvent de suivre les conseils. Cette approche aura aussi pour effet de renforcer l'efficacité et la sécurité des systèmes ainsi que la confiance que le public aura dans l'institution. En outre, ces lignes directrices sont plus qu'une simple collection de bonnes pratiques non contraignantes. Elles contiennent en effet l'interprétation de la législation par le CEPD, qui fait autorité. Le respect des lignes directrices sera pris en considération par le CEPD dans l'éventualité où il serait amené à faire usage de ses prérogatives en matière d'application. Le respect des lignes directrices peut donc contribuer à déterminer si une institution fera l'objet d'une inspection et d'autres mesures visant à faire respecter la loi, par exemple:

- un avertissement ou une admonestation[6];
- un ordre d'effacement de données[7];
- une interdiction de traitement[8]; ou
- un renvoi du dossier devant la «hiérarchie» de l'institution concernée, devant le Parlement, le Conseil, la Commission ou la Cour de justice européenne[9].

2 Champ d'application des lignes directrices

2.1 Champ d'application

Les lignes directrices s'appliquent à la vidéosurveillance pratiquée par les institutions ou par une autre partie au nom de celles-ci à toutes les fins pour lesquelles des caméras capturent des données à caractère personnel telles que définies par le règlement.

Ces lignes directrices se focalisent sur la vidéosurveillance utilisée à des fins typiques de sécurité, y compris le contrôle d'accès. Mais elles s'appliquent également:

- aux opérations de sécurité plus complexes ou plus spécifiques;
- à la vidéosurveillance utilisée dans le cadre d'enquêtes internes (liées ou non à la sécurité); et

[6] Voir l'article 47, paragraphe 1, point d) du règlement.

[7] Article 47, paragraphe 1, point e).

[8] Article 47, point f).

[9] Article 47, paragraphe 1, points g) et h).

- à la vidéosurveillance pratiquée à toute autre fin.

2.2 Exclusions du champ d'application

Ces lignes directrices ne s'appliquent pas aux activités suivantes:

- les appels en vidéophonie et la vidéoconférence;
- les systèmes simples d'entrée vidéo sans enregistrement[10];
- l'utilisation de caméras à des fins artistiques ou journalistiques (par ex. pour réaliser un film ou pour enregistrer ou diffuser des événements notables)[11];
- l'utilisation de caméras à des fins scientifiques dans des environnements contrôlés de laboratoire, pour autant que ces caméras contrôlent uniquement des processus (par ex. des processus physiques ou chimiques) et non des personnes;
- l'enregistrement ou la diffusion d'événements tels que des conférences, séminaires, réunions ou activités de formation à des fins documentaires, de formation ou autres; et
- l'enregistrement ou la diffusion des réunions des organes décisionnels de l'UE en vue d'en renforcer la transparence (par ex. retransmission en direct des séances plénières du Parlement européen).

Ces utilisations et d'autres utilisations potentielles, bien qu'elles tombent peut-être dans le champ d'application et qu'elles nécessitent donc, dans certains cas, des garanties en matière de protection des données, ne sont pas abordées par ces lignes directrices. Les institutions doivent donc évaluer leurs besoins de conformité au cas par cas.

2.3 Clarifications relatives au champ d'application

2.3.1. Les lignes directrices couvrent-elles les dispositifs autres que les systèmes de télévision en circuit fermé (CCTV)?

Aux fins des présentes lignes directrices, la vidéosurveillance est définie comme la surveillance d'un endroit, d'un événement, d'une activité ou d'une personne spécifique au moyen d'un dispositif ou système électronique de représentation visuelle. Les institutions utilisent généralement des systèmes CCTV («closed-circuit

[10] Nous entendons par là un système simple qui permet à une réceptionniste ou à un gardien de sécurité d'ouvrir à distance une porte verrouillée (par ex. une porte principale ou de garage) pour laisser entrer les visiteurs qui ne possèdent pas de badge leur donnant un accès automatique. Ce système est activé par les visiteurs eux-mêmes lorsqu'ils «sonnent» à la porte. Cette exception doit être interprétée dans un sens étroit et ne doit pas s'appliquer à des systèmes plus complexes ni à des systèmes dans lesquels, même si aucun enregistrement n'a lieu, les visiteurs se trouvent dans le champ de couverture des caméras de sécurité sans initier eux-mêmes le contact. Voir l'exemple du chapitre 2.3.4 ci-dessous à titre de comparaison.

[11] Les lignes directrices s'appliquent toutefois à la communication aux médias de séquences de vidéosurveillance enregistrées avec une finalité différente. Voir le chapitre 10 pour le cadre général en matière de transmission.

television» ou télévision en circuit fermé) composés d'une série de caméras surveillant un domaine protégé spécifique, avec un matériel supplémentaire permettant de transférer, de visualiser et/ou de stocker les séquences vidéo à des fins de traitement. L'utilisation de tout autre dispositif ou système, fixe ou mobile, relève toutefois aussi du champ d'application de ces lignes directrices si ce système est capable d'enregistrer des images. C'est le cas, par exemple, des caméras vidéo portables, des appareils photos, des webcams, des caméras à infrarouges et des dispositifs de détection thermique.

2.3.2. Qu'entend-on par «données à caractère personnel»?

Le règlement définit les données à caractère personnel comme «toute information concernant une personne physique identifiée ou identifiable». Le règlement prévoit également qu'«est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale»[12]. Qu'est-ce que cela signifie en pratique?

Tout d'abord, les images montrant un visage reconnaissable constituent toujours des données à caractère personnel. C'est le cas même si les opérateurs du système ne connaissent pas les personnes concernées ou ne les ont pas identifiées.

Exemple:

Votre institution installe des caméras vidéo qui surveillent une salle d'archives fermée à clef la nuit et le week-end dans le but d'enregistrer des images de visages reconnaissables et d'identifier la personne se rendant coupable de tout accès non autorisé. Les lignes directrices sont d'application même si vous avez uniquement enregistré ces images sans jamais visionner les enregistrements.

Cependant, il n'est pas nécessaire d'enregistrer des images de visages reconnaissables pour que les lignes directrices s'appliquent. Des images moins clairement visibles représentant une personne peuvent aussi constituer des données à caractère personnel pour autant que la personne concernée soit identifiable, que ce soit directement ou indirectement (avec l'aide d'autres éléments d'information). Les circonstances de chaque situation déterminent si une personne peut être considérée comme indirectement reconnaissable. Ces circonstances sont, par exemple, l'objectif de la vidéosurveillance et la probabilité que l'institution (ou d'autres destinataires éventuels) soit en mesure de faire les efforts nécessaires pour identifier la personne dont l'image est enregistrée par la caméra.

[12] Voir l'article 2, point a) du règlement et l'avis 4/2007 du Groupe de travail «article 29» sur la protection des données sur le concept de données à caractère personnel, notamment les pages 16 et 21.

Exemple:

Des caméras à faible résolution sont installées sur le toit d'un immeuble pour surveiller la situation générale des alentours à des fins de sécurité lors d'événements exceptionnels. Même si les enregistrements de ces caméras ne contiennent pas toujours des images reconnaissables, la police pourrait, dans le cadre d'une enquête sur un délit grave, être en mesure d'identifier les personnes enregistrées par les caméras en utilisant les informations dérivées du film (par exemple leurs vêtements, silhouette, les objets qu'elles transportent) et d'autres informations obtenues au cours de l'enquête (par exemple à l'aide de témoins ou en utilisant d'autres enregistrements). Dans ces situations, les lignes directrices sont d'application.

En outre, les séquences vidéo contenant des objets susceptibles d'être associés à une personne peuvent également être considérées comme des données à caractère personnel selon les circonstances.

Exemple:

Un système CCTV qui contrôle les plaques minéralogiques de véhicules est connecté à une base de données contenant les données d'immatriculation des véhicules. Ce système possède également un logiciel capable de lire les plaques minéralogiques et de les associer à la personne au nom de laquelle le véhicule est immatriculé. Ce système relève du champ d'application des lignes directrices même si la caméra ne filme pas les personnes, mais uniquement les plaques minéralogiques.

Enfin, les lignes directrices s'appliquent même si l'institution concernée n'a pas l'intention d'enregistrer des images permettant d'identifier les personnes filmées par les caméras, dès lors que ces caméras filment effectivement des personnes identifiables.

Exemple:

Une webcam est installée dans le but de promouvoir un lieu touristique. Les lignes directrices s'appliquent même si l'intention de l'opérateur de cette caméra n'est pas d'identifier les personnes filmées.

2.3.3. Les lignes directrices s'appliquent-elles uniquement aux systèmes de vidéosurveillance permanents?

Non, les lignes directrices s'appliquent même si les caméras sont utilisées uniquement sur une base *ad hoc*.

Exemple:

Après une série de vols, une caméra vidéo est installée à l'entrée d'un local de stockage précédemment non surveillé pendant une période limitée (une semaine) afin de dissuader les voleurs ou de faciliter l'enquête si un vol se produit malgré la présence des caméras. La vidéosurveillance relève du champ d'application des lignes directrices malgré son caractère temporaire et ad hoc.

2.3.4. Les lignes directrices s'appliquent-elles si les images ne sont pas enregistrées?

Oui, la surveillance ou la diffusion en direct relèvent aussi du champ d'application du règlement et des lignes directrices.

Exemple:

Les caméras de sécurité surveillent les sorties et les entrées d'un bâtiment. Les images ne sont pas enregistrées, mais visionnées par le personnel de sécurité dans une salle de contrôle ou à l'accueil du bâtiment. Les lignes directrices sont d'application.

En effet, il peut y avoir des risques pour la sécurité et le respect de la vie privée même si aucune séquence n'est enregistrée et si les images sont uniquement transmises en direct à leurs destinataires via un réseau interne. Il existe, par exemple, un risque que les images soient interceptées par un pirate informatique ou enregistrées puis utilisées à des fins non compatibles par l'un des destinataires. Il est important de noter que l'atteinte à la vie privée et l'impact sur le comportement des sujets surveillés seront souvent comparables à l'atteinte et à l'impact des enregistrements. En général, les risques en matière de vie privée et de protection des données ont tendance à augmenter avec le nombre de destinataires et sont particulièrement élevés si les séquences sont téléchargées sur l'internet.

2.3.5. Que se passe-t-il dans le cas d'une surveillance confiée à une entreprise extérieure?

Si une institution confie une partie ou la totalité de ses activités de vidéosurveillance à une partie tierce (un «**sous-traitant**»), elle reste responsable du respect du règlement en sa qualité de «responsable du traitement».

Exemple:

Les gardiens de sécurité qui contrôlent les séquences vidéo dans le local de réception d'une institution travaillent pour une entreprise privée à laquelle l'institution a confié la surveillance en direct. Dans ce cas, l'institution doit s'assurer que les gardiens de sécurité s'acquittent de leurs responsabilités conformément aux dispositions du règlement et aux lignes directrices.

Pour plus d'orientations concernant l'externalisation, veuillez vous référer au chapitre 14.4 ci-dessous.

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

3.1 Prise en compte du respect de la vie privée dès la conception du système

Idéalement, des garanties de protection des données et de respect de la vie privée doivent être intégrées aux spécifications de conception de la technologie utilisée par les institutions tout comme elles sont prises en compte par les pratiques institutionnelles[13].

3.2 Résoudre les problèmes de protection des données de façon précoce

Lors de l'installation ou de la mise à jour d'un système de vidéosurveillance, il convient de réaliser une évaluation initiale de protection des données avec l'aide du DPD bien avant de lancer un appel d'offre pour de nouveaux achats ou de prendre un quelconque engagement financier. Cette évaluation permettra d'éviter des erreurs coûteuses.

Exemple:

En tant que chef de l'unité chargée de la sécurité de votre institution, vous ressentez la nécessité de mettre à niveau le système de vidéosurveillance existant, ce qui implique l'achat et l'installation de caméras et d'un logiciel supplémentaires. Il est important d'effectuer au moins une analyse préliminaire à un stade précoce, dans la mesure où cette analyse peut non seulement aboutir à l'adoption de mesures spécifiques en matière de protection des données, mais aussi à la modification des spécifications de l'appel d'offre à destination des fournisseurs. Cette analyse pourrait même aboutir à une diminution de l'investissement prévu.

[13] Avis n° 168 du groupe de travail du 1er décembre 2009 sur «L'avenir de la protection de la vie privée», contribution conjointe du groupe de travail «Article 29» sur la protection des données et du groupe de travail «Police et justice» à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel. Voir en particulier le chapitre 4.

3.3 Analyse d'impact

Le CEPD recommande de procéder à une analyse d'impact en matière de protection de la vie privée et des données avant d'installer et de mettre en service des systèmes de vidéosurveillance dans tous les cas où une telle étude contribue aux efforts de conformité de l'institution[14]. L'objectif de l'analyse d'impact est de déterminer l'impact du système envisagé sur le respect de la vie privée des personnes et d'autres droits fondamentaux, mais aussi d'identifier des façons d'atténuer ou d'éviter les éventuels effets négatifs.

Les efforts à consacrer à une analyse d'impact dépendent des circonstances. Un système de vidéosurveillance présentant des risques inhérents importants et un système qui soulève des problèmes complexes et nouveaux nécessite des efforts nettement plus importants qu'un système présentant un impact relativement modeste pour le respect de la vie privée et des autres droits fondamentaux. C'est le cas, par exemple, d'un système CCTV traditionnel utilisé à des fins typiques de sécurité, et pour lequel les lignes directrices assurent déjà des garanties suffisantes.

Quoi qu'il en soit et dans tous les cas, qu'il s'agisse d'une analyse d'impact formelle ou autre, l'institution doit évaluer et justifier la nécessité de recourir à la vidéosurveillance, déterminer l'emplacement des équipements, sélectionner et configurer ses systèmes et déterminer comment elle compte appliquer les garanties de protection des données proposées dans ces lignes directrices.

Il peut également arriver qu'une institution propose un système non conventionnel. Dans ce cas, l'institution concernée doit évaluer soigneusement les différences prévues par rapport aux recommandations énoncées par les lignes directrices, en discuter avec son DPD et avec les autres parties prenantes. Elle doit documenter son évaluation par écrit, sous la forme d'une analyse d'impact formelle ou sous une autre forme. L'audit du système par l'institution (voir le chapitre 13) doit également aborder la légalité de la personnalisation du système.

Enfin, du fait de leur complexité, de leur nouveauté, de leur spécificité ou de leurs risques intrinsèques, le CEPD recommande vivement de réaliser une analyse d'impact pour les systèmes suivants:

- vidéosurveillance à des fins autres que la sécurité (par exemple à des fins d'enquête, voir chapitre 5.8);
- contrôle des employés (chapitre 5.9);
- webcams (chapitre 5.10);
- surveillance sur le territoire d'un État membre et dans des pays tiers (chapitres 6.5-6.6);

[14] En ce qui concerne les systèmes déjà opérationnels à la date d'entrée en vigueur des présentes lignes directrices, l'analyse d'impact doit être réalisée rétroactivement. Voir le chapitre 15 pour de plus amples informations concernant les dispositions transitoires et la façon de garantir la conformité des systèmes existants.

- catégories spéciales de données (chapitre 6.7);
- contrôle de sites où les personnes s'attendent à un respect plus important de leur vie privée (chapitre 6.8);
- vidéosurveillance de haute technologie et/ou intelligente (chapitre 6.9);
- systèmes interconnectés (chapitre 6.10);
- surveillance dissimulée (chapitre 6.11);
- enregistrement sonore et «caméra de surveillance parlante» (chapitre 6.12).

L'analyse d'impact peut être réalisée en interne ou par une société indépendante. L'évaluation doit avoir lieu à un stade précoce du projet. Sur la base des résultats de l'analyse d'impact, une institution peut décider

- de renoncer au contrôle prévu ou de le modifier et/ou
- d'appliquer des mesures de protection supplémentaires en plus de celles recommandées par les lignes directrices.

L'analyse d'impact doit être correctement documentée. En principe, le rapport de l'analyse d'impact doit spécifier clairement les risques pour le respect de la vie privée et/ou les autres droits fondamentaux identifiés par l'institution et les garanties supplémentaires proposées.

Exemple:

Votre institution envisage d'installer un système complexe de vidéosurveillance dynamique et préventive. Cette installation peut n'être admissible que moyennant une analyse complète de l'impact en matière de vie privée et de protection des données par l'institution (et moyennant toutes les autres garanties prévues par ces lignes directrices ou recommandées par le CEPD dans le cadre d'une procédure de contrôle préalable.

3.4 Utiliser des technologies respectueuses de la vie privée

Il y a lieu d'utiliser autant que possible des solutions technologiques respectueuses de la vie privée. Lors de la commande du système et de la rédaction des spécifications d'appel d'offres, les fournisseurs doivent être invités et encouragés à proposer des solutions de ce type.

Exemples:

- Le cryptage des données peut réduire le préjudice potentiel en cas d'accès non autorisé aux données. Voir également le chapitre 9 ci-dessous.
- Masquer ou brouiller les images afin d'éviter la surveillance d'endroits sans relation avec l'objet de votre surveillance. Cette technique est également utile pour supprimer les images de personnes tierces lorsque vous donnez accès aux images d'une personne concernée. Voir aussi l'utilisation de cette technique pour protéger les visages ou les plaques minéralogiques en cas d'utilisation d'une webcam (chapitre 5.10).

3.5 Planifier pour une surveillance ad hoc

Enfin, l'institution qui envisage d'utiliser la vidéosurveillance sur une base ad hoc (par exemple lors de l'organisation d'événements importants ou dans le cadre d'enquêtes internes) doit également dresser des plans à l'avance. Dans ce cas, le cadre et les politiques nécessaires pour la protection des données doivent être mis en place suffisamment longtemps avant la vidéosurveillance elle-même.

Exemples:

- *Votre institution accueille régulièrement des événements importants tels que des réunions de chefs d'État ou de gouvernement, qui nécessitent un renforcement de la sécurité.*
- *Vous prévoyez qu'il faudra parfois installer et utiliser des caméras dans le cadre d'enquêtes internes. Ces caméras seront installées à certains endroits, pour une période limitée et sur une base ad hoc.*

4 Qui consulter à propos du nouveau système?

Il est essentiel de consulter les parties prenantes et les autorités compétentes afin d'identifier tous les problèmes possibles en matière de protection des données. Au moment de décider d'utiliser ou non la vidéosurveillance et de mettre en place le cadre et les politiques nécessaires pour la protection des données, il peut être nécessaire de consulter les personnes ou les organisations suivantes, ou en tout cas certaines d'entre elles:

- le DPD de l'institution;
- les représentants des employés;
- d'autres parties prenantes (y compris, dans certains cas, les autorités locales);
- le CEPD; et
- les autorités nationales (ou régionales) de protection des données.

4.1 Délégué à la protection des données

Avant tout, les projets d'installation ou de mise à jour d'un système de

vidéosurveillance doivent être communiqués au DPD de l'institution. Le DPD doit être consulté systématiquement et impliqué à toutes les étapes du processus décisionnel.

Exemples:

- *Le DPD doit participer à la décision initiale d'utiliser ou non la vidéosurveillance, comme mentionné au chapitre 3.2.*
- *Le DPD doit être invité à fournir des avis d'expert sur l'élaboration de procédures respectueuses de la protection des données.*
- *Le DPD doit être invité à commenter le projet de politique de vidéosurveillance de l'institution (y compris ses annexes), à corriger les erreurs et à proposer des améliorations.*
- *Il est recommandé de demander l'aide du DPD dans vos communications avec le CEPD et les autorités nationales (ou régionales) de protection des données.*

4.2 Personnel et autre parties prenantes

Le CEPD recommande vivement de consulter le personnel dans tous les cas où des membres du personnel sont susceptibles d'être filmés. Cette consultation est recommandée même si le traitement des images n'a pas pour but de contrôler ni d'évaluer le travail des membres du personnel. Cette consultation est obligatoire dans les cas où la législation en vigueur l'impose. Le personnel peut être consulté par l'intermédiaire des comités actifs au sein de l'institution, mais d'autres approches (par exemple des consultations publiques et des ateliers) peuvent aussi être efficaces.

Exemple:

Il convient de consulter le personnel même si la vidéosurveillance est utilisée uniquement à des fins de sécurité et de contrôle des accès, et même si les caméras sont installées uniquement aux entrées et aux sorties des bâtiments et dans certains autres endroits stratégiques tels que les salles d'archives.

La consultation ne signifie pas que la direction doive toujours conclure un accord avec les représentants du personnel concernant l'ampleur du contrôle. Le CEPD estime cependant qu'une consultation véritable constitue une garantie particulièrement importante que le système de vidéosurveillance installé ne sera pas plus inquisiteur que nécessaire et que des mesures de protection adéquates seront prises pour réduire le plus possible les risques pour la vie privée, les autres droits fondamentaux et les intérêts légitimes du personnel.

Si l'emplacement ou la nature du système de vidéosurveillance fait que d'autres parties prenantes sont concernées, l'institution doit veiller à ce que ces parties prenantes ou leurs représentants soient eux aussi consultés le plus largement possible. Il convient notamment de consulter les pouvoirs locaux, la police ou

d'autres organes dans les cas décrits aux chapitres 6.5 et 6.6.

Exemple:

Il y a lieu de consulter les parents dans les cas où la vidéosurveillance couvre l'infrastructure d'accueil des enfants utilisée par votre institution.

4.3 Contrôle préalable par le CEPD

Dans certains cas, le DPD de l'institution doit soumettre une notification de contrôle préalable au CEPD[15]. L'objectif de cette procédure est d'aider l'institution à mettre en place des garanties supplémentaires de protection des données dans les cas où ses activités vont au-delà des formes de vidéosurveillance pour lesquelles les lignes directrices apportent déjà des garanties suffisantes. Au cours de la procédure de contrôle préalable, le CEPD pourra également vérifier le respect par l'institution des recommandations émises par les lignes directrices.

Le CEPD considère qu'une notification de contrôle préalable est requise dans les cas suivants:

- vidéosurveillance envisagée à des fins d'enquête (chapitre 5.8);
- contrôle des employés (chapitre 5.9);
- traitement de catégories spéciales de données (chapitre 6.7);
- contrôle de sites où les personnes s'attendent à un respect plus important de leur vie privée (chapitre 6.8);
- vidéosurveillance de haute technologie et/ou intelligente (chapitre 6.9);
- systèmes interconnectés (chapitre 6.10);
- surveillance dissimulée (chapitre 6.11);
- enregistrement sonore et «caméra de surveillance parlante» (chapitre 6.12).

La notification doit inclure le rapport de l'analyse d'impact (ou toute autre documentation utile relative à l'analyse d'impact), la politique de vidéosurveillance et le rapport d'audit (voir le chapitre 13 ci-dessous).

4.4 Autorités nationales de protection des données

Les dispositions du règlement sont d'application[16] et le CEPD est compétent pour contrôler toutes les formes de vidéosurveillance pratiquées par ou au nom des institutions, que les images soient filmées à l'intérieur des bâtiments des institutions ou en dehors de ceux-ci. Ceci étant, les autorités de protection des données de l'État membre dans lequel une institution est installée peuvent également s'intéresser à la

[15] Voir l'article 27 du règlement, qui stipule que «[L]es traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités sont soumis au contrôle préalable du contrôleur européen de la protection des données».

[16] Voir les articles 3, paragraphe 1 et 41, paragraphe 2 du règlement.

surveillance organisée à l'extérieur des bâtiments. Dans ce cas, l'applicabilité de la législation nationale en matière de protection des données est limitée par les privilèges et immunités des institutions conformément à l'article 291 TCE et au protocole (n° 36) relatif aux privilèges et immunités des Communautés européennes (1965) [17]. Le CEPD collaborera au besoin avec les autorités de protection des données des États membres[18].

Le chapitre 6.5 contient une série de recommandations visant à réduire le plus possible la surveillance sur le territoire d'un État membre. Ces recommandations devraient encourager l'adoption de bonnes pratiques de protection des données, mais aussi empêcher ou réduire au minimum la duplication des efforts et l'incertitude qui peuvent apparaître du fait de l'applicabilité simultanée de deux régimes de protection des données et de l'action concurrente de deux autorités de contrôle.

En matière de procédure, et en plus de ces recommandations sur le fond, le CEPD recommande aux institutions d'envoyer systématiquement un bref courrier à l'autorité nationale de protection des données (et/ou à l'autorité régionale de protection des données, le cas échéant) lors de la consultation initiale. Dans cette lettre, l'institution doit informer l'autorité concernée qu'elle utilise un système de vidéosurveillance à l'intérieur de ses bâtiments à des fins de sécurité et de contrôle des accès et que ce système enregistre aussi certaines images aux environs de ses bâtiments. Le courrier doit confirmer que ces pratiques sont conformes aux dispositions des présentes lignes directrices et du règlement, et qu'elles sont soumises à l'autorité de contrôle du CEPD (et, le cas échéant, qu'elles feront l'objet d'un contrôle préalable de la part du CEPD). Il doit également contenir un lien vers les lignes directrices ou une copie de celles-ci. Si l'autorité nationale de protection des données demande des informations supplémentaires, l'institution doit coopérer de bonne foi. En cas de contrôle préalable par le CEPD, il est également de bonne pratique d'envoyer l'avis définitif du CEPD à l'autorité de protection des données compétente.

5 Décider d'utiliser - ou non - la vidéosurveillance

La décision d'utiliser un système de vidéosurveillance ne doit pas être prise à la légère et nécessite une évaluation minutieuse des avantages potentiels et de l'impact du système sur le droit à la vie privée et sur d'autres droits fondamentaux et intérêts légitimes des personnes présentes sur le site couvert par le système. La décision doit être documentée par écrit autant que possible et motivée par des données concrètes, par exemple par des données statistiques concernant le nombre d'incidents de sécurité survenus par le passé et des preuves de l'efficacité des caméras pour prévenir ces incidents ou pour faciliter l'enquête et les poursuites après de tels incidents. L'audit doit vérifier l'existence d'une justification écrite de l'utilisation de la vidéosurveillance et en évaluer le caractère adéquat (voir chapitre 13).

[17] Journal officiel C 321 E, 29.12.2006, pp. 0318-0324. On notera que certains «accords de siège» conclus entre les institutions et leurs pays hôtes stipulent explicitement que la législation nationale en matière de protection des données ne s'applique pas aux institutions. C'est le cas par exemple de la Banque centrale européenne.

[18] Voir l'article 28, paragraphe 6 de la directive et l'article 46, point f) du règlement.

Cette analyse ne doit cependant pas consister systématiquement en un processus long ou complexe. La portée de l'évaluation dépend de la taille du système proposé et du niveau d'impact qu'il est susceptible d'avoir sur la vie privée, les autres droits fondamentaux ou les intérêts légitimes des personnes concernées. Dans leur évaluation, les institutions doivent apporter une réponse aux questions suivantes:

- Quels sont les avantages attendus de la vidéosurveillance, et ces avantages sont-ils suffisants pour compenser ses effets négatifs?
- L'objectif du système est-il clairement spécifié, explicite et légitime? Existe-t-il une base légale pour la vidéosurveillance?
- La nécessité d'utiliser la vidéosurveillance a-t-elle été clairement démontrée? La vidéosurveillance est-elle l'outil qui convient pour obtenir le résultat attendu, et existe-t-il des alternatives moins intrusives?

Les orientations contenues dans ce document aideront les institutions à déterminer dans quels cas l'utilisation de la vidéosurveillance est indiquée. En ce qui concerne les systèmes existants[19], de nombreuses institutions constateront probablement qu'elles doivent simplement se montrer plus explicites et transparentes, et confirmer par écrit les bonnes pratiques déjà en place.

5.1 Objectif du système

Avant de décider d'installer un nouveau système, l'institution doit d'abord déterminer l'objectif de la vidéosurveillance et s'assurer de la légitimité de cet objectif[20].

5.1.1 Être clair, spécifique et explicite. Une description vague, ambiguë ou tout simplement trop générale ne suffit pas. Une description spécifique et précise de l'objectif de la vidéosurveillance peut aider l'institution concernée à respecter la loi, à évaluer l'efficacité de son système et à expliquer à son personnel et au grand public pourquoi ce système est nécessaire.

5.1.2. Communiquer l'objectif au public. L'objectif du système doit être communiqué au public sous une forme sommaire à l'endroit concerné, et sous une forme plus détaillée, par exemple, via une version publique en ligne de la politique de vidéosurveillance de l'institution[21].

5.1.3. Utilisation incompatible et détournement d'usage[22]. Les restrictions d'utilisation des données doivent être clairement définies, surtout si les représentants du personnel ou d'autres parties prenantes en font la demande.

---

[19] Voir le chapitre 15 consacré aux dispositions transitoires.

[20] Voir le règlement, article 4, point b).

[21] Voir le chapitre 11 et les annexes 1 et 2 pour plus de conseils sur la façon de communiquer cette information au public.

[22] Voir l'article 4, point b) du règlement concernant l'utilisation à des fins incompatibles.

Il convient en outre de s'assurer que ces données ne sont pas utilisées ultérieurement à des fins non prévues, ni divulguées à des destinataires non prévus qui pourraient l'utiliser à des fins supplémentaires et incompatibles («**détournement d'usage**»). Les objectifs incompatibles comprennent non seulement les objectifs nouveaux sans aucun lien avec la finalité initiale, mais aussi tous les objectifs auxquels la personne surveillée ne pouvait pas raisonnablement s'attendre. Une définition large et de haut niveau de la finalité du système ne justifie pas son utilisation ultérieure à des fins non précisées.

Exemple:

Lorsqu'un système de vidéosurveillance est installé à des fins de sécurité, et annoncé comme tel au personnel, les enregistrements ne peuvent pas être utilisés pour évaluer le travail des membres du personnel ni pour vérifier s'ils arrivent à l'heure. Ces données ne peuvent pas non plus être utilisées à des fins d'enquête ni comme preuves dans le cadre d'enquêtes internes ou de procédures disciplinaires, sauf dans le cas d'un incident de sécurité physique ou, dans des cas exceptionnels, de comportement criminel.

5.2 Existe-t-il une base légale pour la vidéosurveillance[23]?

Si une institution utilise la vidéosurveillance à des fins typiques de sécurité et de contrôle des accès, on peut considérer que cette pratique est *potentiellement* nécessaire pour la gestion et le fonctionnement de cette institution. À ce titre, le système de vidéosurveillance est légitime conformément aux exigences du règlement[24].

Si tel n'est pas le cas, il faut se demander s'il existe une autre base légale possible pour la vidéosurveillance. La vidéosurveillance peut également être légitime en cas d'obligation légale de pratiquer une vidéosurveillance, ou dans les cas où les personnes concernées ont indubitablement donné leur consentement[25].

5.3 La nécessité d'utiliser la vidéosurveillance a-t-elle été clairement démontrée?

Une fois que l'objectif du système de vidéosurveillance a été défini et que sa licéité a été vérifiée, il reste à démontrer que l'utilisation de caméras est effectivement *nécessaire* compte tenu des circonstances spécifiques de l'institution[26].

---

[23] Voir l'article 5 du règlement.

[24] Voir l'article 5, point a) et le considérant 27 du règlement.

[25] Voir l'article 5, points b) et d).

[26] Voir le règlement, article 5, points a), b), c) et e). (Si la vidéosurveillance est basée sur le

5.4 La vidéosurveillance est-elle un outil efficace pour réaliser les objectifs?

Il ne faut pas installer de système de vidéosurveillance dans les cas où ce système ne permettra pas d'atteindre l'objectif attendu, par exemple s'il donne uniquement l'illusion d'une meilleure sécurité.

Exemple:

Si l'objectif de votre système est de contrôler l'accès à différentes parties d'un grand bâtiment qui ne sont pas séparées physiquement par des portes verrouillées ou par d'autres systèmes de contrôle des accès, l'utilisation d'une centaine de caméras dont les enregistrements sont visionnés depuis une salle de contrôle par deux opérateurs de CCTV ne vous aidera pas à empêcher les accès non autorisés. Dans le meilleur des cas, ce système pourra uniquement vous aider à enquêter sur un incident de sécurité après les faits.

5.5 Des alternatives moins intrusives sont-elles disponibles?

L'institution doit également évaluer la possibilité d'utiliser une méthode moins intrusive pour atteindre l'objectif recherché sans avoir recours à des caméras. Si des alternatives adéquates sont disponibles, il est préférable de ne pas utiliser la vidéosurveillance. Une alternative peut être considérée comme adéquate sauf si elle n'est pas réalisable, si elle est nettement moins efficace que la vidéosurveillance ou si elle implique un surcoût disproportionné.

Le simple fait que la technologie soit disponible à un prix relativement peu élevé ne suffit pas à justifier l'utilisation de la vidéosurveillance. Il convient d'éviter de prendre simplement la décision qui semble la moins chère, la plus facile et la plus rapide sans prendre en considération son impact sur les intérêts légitimes des personnes concernées et sur leurs droits fondamentaux.

Exemple:

Vous ne devez pas installer un système de vidéosurveillance pour surveiller la partie de vos centres informatiques offrant un accès à l'internet à vos visiteurs dans le seul but d'évaluer le nombre de places disponibles. Une alternative possible consiste à installer un logiciel qui permet de connaître à tout moment le nombre d'ordinateurs connectés et déconnectés dans chaque centre informatique.

---

consentement, vous devez vous assurer que cette vidéosurveillance ne va pas au-delà de ce qui est nécessaire pour atteindre l'objectif auquel les personnes concernées ont donné leur consentement.)

5.6 Les avantages sont-ils suffisants pour compenser les effets négatifs[27]?

Enfin, même si une institution arrive à la conclusion qu'il existe un besoin réel d'utiliser la vidéosurveillance et qu'il n'existe pas d'autre méthode moins intrusive, elle ne doit avoir recours à cette technologie que si les effets négatifs de la vidéosurveillance sont compensés par ses avantages.

Il va de soi que la vidéosurveillance ne doit pas être utilisée dans les cas où cette mesure est clairement disproportionnée par rapport aux bénéfices escomptés.

Exemple:

Vous ne devez pas installer une caméra dans la cuisine commune pour détecter les personnes qui «empruntent» des articles placés dans le réfrigérateur ou les armoires par d'autres membres du personnel, même si (i) la présence de la caméra est signalée; (ii) le problème est récurrent; et (iii) d'autres tentatives de régler le problème ont échoué.

Dans de nombreux cas cependant, l'analyse s'avère plus complexe et il faut trouver un équilibre difficile entre les intérêts légitimes et les droits fondamentaux des personnes concernées et les bénéfices escomptés de la vidéosurveillance.

5.7 Objectifs de sécurité

Si la vidéosurveillance est pratiquée à des fins de sécurité, l'institution concernée doit évaluer soigneusement les risques et ne pas se contenter d'affirmer que la finalité du système est d'«observer les anomalies à l'intérieur du périmètre de sécurité» ou de «régler les incidents de sécurité». L'institution ne doit pas se contenter d'avoir une idée générale de la finalité de son système. Elle doit au contraire décrire en détail les types d'incidents de sécurité susceptibles de se produire sur le site surveillé et dont elle espère que l'utilisation de caméras permettra de les dissuader, de les empêcher, de faciliter l'enquête après coup ou la poursuite des coupables.

De façon générale, au moment de définir la finalité du système, l'institution doit indiquer clairement que le système de vidéosurveillance facilite le contrôle des accès à ses bâtiments et qu'il contribue à garantir la sécurité des bâtiments, la sécurité du personnel et des visiteurs ainsi que l'intégrité des biens et des informations présents dans les locaux.

Elle doit également préciser si le système de vidéosurveillance est conçu pour

[27] Voir l'article 4, paragraphe 1, point c) du règlement et les articles 8 et 52 de la Charte des droits fondamentaux de l'Union européenne. Parmi les autres dispositions pertinentes en matière de droits fondamentaux, on peut citer notamment les articles 7, 11, 12, 21 et 45 de la Charte. Voir également la Convention européenne des droits de l'homme, et notamment ses articles 8, 10 et 11 et son protocole 4, article 2, ainsi que l'article 13 du Traité instituant les Communautés européennes.

empêcher et dissuader les incidents de sécurité et/ou pour faciliter les enquêtes et les poursuites en cas d'incident (en constituant des preuves) [28].

Elle ne doit pas seulement identifier tous les risques de sécurité possibles, mais aussi démontrer, de façon réaliste et vérifiable, l'existence et l'ampleur de ces risques (dangers spécifiques, taux de criminalité, etc.). La simple «perception» d'un risque, la spéculation et les anecdotes ne suffisent pas à démontrer la nécessité de la vidéosurveillance. Cette analyse des risques doit être documentée par écrit et doit identifier et évaluer tous les risques existants. L'institution doit démontrer les risques de sécurité présents sur le site surveillé en décrivant les incidents de sécurité qui s'y sont produits par le passé ou qui risquent de s'y produire à l'avenir.

Exemples:

Vous devez envisager et évaluer spécifiquement et individuellement l'utilisation de la vidéosurveillance pour chacun des types d'incidents de sécurité suivants, selon les circonstances:

- *accès physique non autorisé à des locaux sécurisés spécifiques et à des pièces protégées (par ex. pièces abritant des infrastructures informatiques critiques ou des informations opérationnelles sensibles);*
- *vol d'objets personnels appartenant à des membres du personnel (par ex. ordinateurs portables, téléphones mobiles, sacs à main, vestes laissés sans surveillance dans des bureaux ou des salles de réunion);*
- *vols de vélos ou effractions de voitures sur votre parking;*
- *menaces de sécurité lors de sommets internationaux ou d'autres événements particuliers;*
- *pannes de matériel dans des laboratoires de recherches nucléaires;*
- *attaques physiques contre vos bâtiments (jets de pierres, effractions, vandalisme, etc.) lors de protestations et de manifestations;*
- *agression physique de votre personnel de sécurité à l'entrée principale lors de protestations et de manifestations.*

La liste ci-dessus est purement indicative.

Une fois les risques identifiés, il convient de poser une série plus complète de questions non seulement pour établir l'existence de menaces spécifiques, mais aussi pour démontrer que la vidéosurveillance est l'outil qui convient pour contrer ces menaces. Comme indiqué aux chapitres 5.4 - 5.6, il convient de démontrer que la vidéosurveillance est un outil efficace pour atteindre l'objectif, qu'il n'existe pas de

[28] La vidéosurveillance peut parfois contribuer à empêcher les incidents de sécurité, que ce soit en dissuadant les coupables potentiels ou en permettant une réaction rapide dans les situations d'urgence. Dans la pratique toutefois, plutôt que de prévenir les incidents de sécurité, la vidéosurveillance n'est souvent utilisée que dans le cadre d'enquêtes ultérieures, pour fournir des preuves après un incident. Vous devez indiquer clairement les objectifs recherchés.

solution alternative moins intrusive et que les avantages compensent les effets négatifs. Avant d'opter pour la vidéosurveillance, il est important d'envisager soigneusement toutes les alternatives moins intrusives. Il peut s'agir, par exemple, de contrôles effectués par le personnel de sécurité, d'une mise à niveau des systèmes d'alarme, de systèmes de contrôle d'accès, de l'installation de barrières, portes et fenêtres blindées et renforcées ou encore d'un meilleur éclairage. La vidéosurveillance ne doit être utilisée que si l'insuffisance de ces solutions a été démontrée.

5.8 Utilisation à des fins d'enquête

Lorsqu'un système est mis en place à des fins typiques de sécurité, les enregistrements vidéo peuvent servir à enquêter sur les incidents physiques de sécurité, par exemple l'accès non autorisé aux locaux ou à des pièces protégées, le vol, le vandalisme, un incendie ou l'agression physique d'une personne. Outre la dissuasion et la prévention, les systèmes de vidéosurveillance sont presque toujours destinés à faciliter l'enquête après un incident de sécurité et à apporter des preuves permettant de poursuivre le coupable. En principe toutefois, les systèmes de vidéosurveillance ne doivent pas être installés ou conçus à des fins d'enquêtes internes dépassant le cadre des incidents de sécurité tels que ceux décrits ci-dessus.

Ceci étant dit, il n'est pas exclu que dans des circonstances exceptionnelles, la technologie de vidéosurveillance puisse servir à des fins d'enquête sans lien direct avec un incident physique de sécurité. Une analyse au cas par cas est nécessaire pour déterminer si cette utilisation est permissible et si elle nécessite des garanties supplémentaires qui ne sont pas prévues par les présentes lignes directrices. Votre politique relative à toute proposition de vidéosurveillance de ce type doit donc faire l'objet d'une analyse d'impact par votre institution et d'un contrôle préalable par le CEPD.

Exemples:

- *Des caméras sont installées dans une salle d'archives verrouillées à des fins de sécurité et de contrôle d'accès, et les images sont visionnées en direct par le gardien de sécurité à la réception. Les images sont également enregistrées. Le système d'alarme se déclenche à 4 heures du matin, signalant un accès non autorisé. L'enquête menée ensuite sur cet incident de sécurité utilise les images du système CCTV. Celles-ci révèlent que la veille, des réparations avaient été effectuées sur le système de climatisation de la salle d'archives et qu'une fenêtre avait été ouverte et laissée ouverte par mégarde. Cette enquête est appropriée et conforme à une finalité typique de sécurité.*

- *Vous souhaitez utiliser le système CCTV de façon ciblée afin d'enquêter sur les activités quotidiennes de M. X, un fonctionnaire de votre institution soupçonné d'avoir fraudé dans le cadre de marchés publics, d'avoir obtenu frauduleusement certains avantages, d'avoir harcelé un(e) collègue de travail ou d'avoir été en état d'ébriété au travail. Cette utilisation dépasse la finalité de sécurité et de contrôle d'accès, et nécessite aussi bien une analyse d'impact qu'un contrôle préalable.*

5.9 Contrôle des employés

Les mesures de contrôle exagérément intrusives peuvent causer un stress inutile aux employés et éroder leur confiance dans l'organisation. Il convient donc d'éviter le recours à la vidéosurveillance pour contrôler le travail du personnel, sauf dans des circonstances exceptionnelles où l'institution concernée démontre qu'elle a un intérêt impérieux à pratiquer cette surveillance.

Tout projet de vidéosurveillance de ce type doit donc faire l'objet d'une analyse d'impact par l'institution concernée. L'institution doit également soumettre ses projets au CEPD en vue d'un contrôle préalable. Dans les cas où une institution envisage de recourir à la vidéosurveillance pour contrôler le travail de son personnel, le CEPD accorde une attention particulière aux opinions et préoccupations exprimées par les représentants du personnel de cette institution et vérifie que ces points de vue ont été pris en considération.

De façon générale, des objectifs tels que la gestion de la productivité du lieu de travail, le contrôle de qualité, le respect des règlements des institutions ou l'obtention de preuves en vue du règlement de litiges ne justifient pas la vidéosurveillance d'employés dans le contexte du travail des institutions.

Exemple:

Vous ne devez pas utiliser votre système de vidéosurveillance existant pour vérifier l'efficacité des agents de nettoyage externes pendant l'accomplissement de leur travail tôt le matin, même si ces personnes ont été correctement informées de cette surveillance et si la qualité de leur travail a fait l'objet de plaintes récurrentes.

Il convient également d'éviter les pratiques qui placent un employé sous une surveillance constante (l'employé est en permanence dans le champ de vision des caméras de vidéosurveillance).

Exemple:

Vous ne devez pas utiliser de caméras de vidéosurveillance pour surveiller en permanence le caissier/la caissière et la caisse de la cantine pendant les heures d'ouverture, même si la personne concernée en a été correctement informée.

En ce qui concerne la surveillance justifiée par des préoccupations de sécurité ou de santé et de sûreté, ou par des intérêts essentiels similaires dans des circonstances exceptionnelles, le CEPD évalue ces justifications au cas par cas.

5.10 Webcams

Aux fins des présentes lignes directrices, on entend par «webcam» un dispositif numérique de saisie d'images vidéo connecté à l'internet et dont les images peuvent être visionnées par toute personne ayant accès au site internet concerné. Les dispositifs reliés à l'intranet d'une institution, ou à des sites internet dont l'accès est limité à un public spécifique (par exemple aux participants à un événement) sont également considérés comme des webcams aux fins des présentes lignes directrices.

Les webcams offrent des possibilités en matière d'éducation, de communication et de loisirs. Mais elles peuvent aussi présenter des risques spécifiques en termes de protection des données. Nombre de ces risques sont liés à la difficulté, pour l'opérateur de la webcam, de déterminer qui visionnera ces images et dans quel but. Les webcams saisissent et transmettent des images numériques qui sont diffusées instantanément à un grand nombre de destinataires. N'importe lequel de ces destinataires peut facilement enregistrer, copier et distribuer ces images à d'autres personnes. Il est alors possible d'enregistrer et d'indexer des enregistrements numériques contenant des informations continues et détaillées, ce qui permet de faire des recherches sur ces dossiers, de repasser les images à l'infini et de les analyser. Les séquences vidéo enregistrées aujourd'hui pourraient rester accessibles en ligne pendant de nombreuses années, et donner ainsi une «empreinte numérique» des personnes concernées. Il y a finalement un risque accru d'utilisation abusive de ces images.

Ces risques se justifient rarement par rapport aux avantages présumés de l'utilisation de webcams - qui dépassent rarement le stade du «divertissement» pur et simple. Il existe aussi bien souvent des alternatives faciles d'accès et moins intrusives pour arriver au même résultat. C'est pourquoi l'installation de webcams doit toujours être mûrement réfléchie. Il faut éviter d'installer des webcams pour des raisons frivoles, ou pour promouvoir des infrastructures de loisirs mises à disposition par l'institution ou un lieu touristique (par ex. le centre des visiteurs, le centre de fitness, la cafétéria, la tribune des visiteurs dans une salle de réunion).

Dans des cas exceptionnels, l'utilisation de webcams peut malgré tout être permissible moyennant le consentement informé de chacun des utilisateurs de l'infrastructure concernée. Il convient d'accorder une attention particulière aux opinions et préoccupations exprimées par les représentants du personnel et/ou d'autres parties concernées.

Exemple:

Vous souhaitez promouvoir un nouveau centre destiné aux visiteurs en installant une caméra vidéo dans le local en question et en diffusant ces images en direct sur le site internet de votre institution. Le CEPD déconseille cette pratique, car de nombreuses personnes risquent de trouver la présence des caméras envahissante. Si par contre une proportion importante des personnes concernées exprime leur intérêt à être filmées, vous pouvez recourir à cette pratique moyennant le consentement clair et informé de chacun des utilisateurs. Les personnes qui utilisent l'infrastructure doivent rester libres de choisir d'utiliser la partie du site couverte par les caméras ou de rester hors champ tout en bénéficiant de façon égale des infrastructures.

Dans la pratique, cela signifie que: (i) seule une (petite) partie de l'infrastructure ainsi promue doit être couverte par les caméras; (ii) les utilisateurs présents dans les autres parties de l'infrastructure doivent pouvoir profiter des infrastructures aux mêmes conditions que dans la zone filmée; et (iii) la zone filmée doit être signalée de façon claire et parfaitement visible. Dans ce cas, le fait d'utiliser la partie du local clairement identifiée comme étant sous l'œil des caméras peut constituer un consentement implicite.

Un autre facteur important à prendre en considération lors de la conception d'un système est la possibilité/facilité d'identification des personnes concernées: une vue aérienne générale d'un bâtiment en basse résolution est nettement moins intrusive que des images permettant de reconnaître le visage des personnes. Il est parfois possible d'atténuer l'impact négatif en matière de vie privée en utilisant un logiciel qui masque les détails susceptibles de faciliter l'identification d'une personne (par ex. les visages ou les plaques minéralogiques). Aucune de ces mesures de protection ne justifie à elle seule l'utilisation de webcams, mais elles doivent intervenir dans la décision d'utiliser ou non de webcams.

6 Choix, emplacement et configuration du système de vidéosurveillance

Ce chapitre propose des conseils concernant le choix, l'emplacement et la configuration d'un système. Le principe fondamental commun à toutes les recommandations contenues dans ce chapitre (et d'ailleurs dans le reste des lignes directrices) est qu'il faut réduire le plus possible tout impact négatif sur le respect de la vie privée et sur les autres droits fondamentaux et intérêts légitimes des personnes surveillées[29]. L'audit doit évaluer et vérifier l'adéquation de chaque décision prise (voir le chapitre 13).

6.1 Emplacement des caméras et angles de vue

Les caméras doivent être placées de façon à filmer le moins possible des endroits inutiles pour l'objectif recherché.

Exemples:

- *Lorsqu'une caméra est montée sur un toit pour surveiller une issue de secours, il convient de veiller à ce qu'elle ne soit pas placée de façon à filmer en même temps la terrasse d'un immeuble privé voisin.*
- *De même, lorsqu'une caméra est installée de façon à surveiller l'entrée d'une pièce bénéficiant d'une protection spécifique à l'intérieur d'un bâtiment, il convient de veiller à ce qu'elle ne soit pas placée de façon à filmer en même temps l'entrée d'un bureau privé voisin.*

En règle générale, lorsqu'un système de vidéosurveillance est installé dans le but de protéger les actifs (biens ou informations) de l'institution ou la sécurité de son personnel et de ses visiteurs, l'institution doit limiter la surveillance:

- à des endroits soigneusement sélectionnés contenant des informations sensibles, des articles de valeur ou d'autres biens nécessitant une protection accrue pour une raison spécifique;
- aux points d'entrée et de sortie des bâtiments (y compris les issues de secours ainsi que les murs et clôtures entourant le bâtiment ou le terrain); et
- aux points d'entrée et de sortie à l'intérieur du bâtiment reliant différentes zones soumises à des droits d'accès différents et séparées par des portes verrouillées ou par un autre mécanisme de contrôle d'accès.

[29] Voir l'article 4, paragraphe 1, point d) du règlement.

Exemples:

- *Vous pouvez installer des caméras à l'entrée d'une salle d'archives verrouillée dans laquelle vous entreposez les documents importants de votre institution et auquel le personnel n'accède que de façon occasionnelle pour archiver ou récupérer des documents.*
- *Vous louez le dernier étage de votre bâtiment à une autre institution. Cet étage est sécurisé par une porte qui est verrouillée en permanence et qui ne s'ouvre qu'au moyen des badges des personnes travaillant au dernier étage. Vous pouvez installer une caméra aux accès à l'ascenseur de cet étage afin de détecter toute personne quittant cet étage ou y accédant depuis un autre endroit du bâtiment.*

Il se peut que les besoins de sécurité nécessitent une surveillance plus poussée à l'intérieur de certains bâtiments. Dans ce cas, ces projets doivent être abordés spécifiquement dans la politique de vidéosurveillance et l'institution doit apporter la preuve de ce besoin et démontrer le caractère proportionnel de la surveillance supplémentaire (via une analyse d'impact ou de toute autre façon).

6.2 Nombre de caméras

Le nombre de caméras à installer dépend de la taille des bâtiments et des besoins de sécurité, qui dépendent eux-mêmes de différents facteurs. Le nombre et le type de caméras qui conviennent à une institution peuvent être tout à fait disproportionnés pour une autre institution. Cependant, toutes choses égales par ailleurs, le nombre de caméras est un bon indicateur de la complexité et de la taille d'un système de surveillance et peut indiquer des risques accrus pour le respect de la vie privée et d'autres droits fondamentaux. L'augmentation du nombre de caméras augmente également le risque que ces caméras ne soient pas utilisées efficacement et que le système provoque une surcharge d'informations. Le CEPD recommande donc de limiter le nombre de caméras au strict nécessaire pour réaliser les objectifs du système. La politique de vidéosurveillance doit préciser le nombre de caméras.

6.3 Horaires de surveillance

Les horaires d'enregistrement des caméras doivent être déterminés de façon à couvrir le moins possible de moments où l'enregistrement ne présente aucun intérêt pour l'objectif recherché. Si l'objectif de la vidéosurveillance est la sécurité, le système doit si possible enregistrer uniquement aux heures présentant une probabilité accrue de problèmes de sécurité.

Exemple:

Des vols sont commis régulièrement la nuit et le week-end dans une salle de rangement verrouillée donnant sur un corridor fort fréquenté. Vous pouvez installer une caméra à proximité de cette salle de rangement afin de détecter les auteurs des vols ou de les empêcher (moyennant une information suffisante). La caméra doit être programmée de façon à fonctionner uniquement en dehors des heures de bureau.

6.4 Résolution et qualité d'image

Il convient d'opter pour une résolution et une qualité d'image adéquates. La qualité d'image requise varie en fonction de l'objectif poursuivi. Si l'identification de personnes est essentielle, par exemple, il convient de prendre en considération la résolution des caméras, les paramètres de compression des systèmes numériques, l'emplacement, l'éclairage et d'autres facteurs et de les définir ou de les modifier de façon à obtenir des images de qualité suffisante pour permettre la reconnaissance des visages. Lorsque l'identification n'est pas nécessaire par contre, la résolution des caméras et les autres paramètres modifiables doivent être choisis de façon à ne pas enregistrer d'images faciales reconnaissables.

Exemple:

Dans certaines situations, l'identification des personnes n'est pas nécessaire et il suffit que la qualité des images permette de détecter les mouvements des personnes ou le flux de la circulation.

6.5 Surveillance sur le territoire d'un État membre

En cas de besoins démontrés de sécurité, une institution peut surveiller les environs immédiats de ses bâtiments sur le territoire des États membres. Il convient toutefois de s'assurer que cette surveillance est réduite au minimum nécessaire pour satisfaire les besoins de sécurité de l'institution. Elle peut couvrir les points d'entrée et de sortie des bâtiments, y compris les issues de secours ainsi que les murs et clôtures entourant le bâtiment ou le terrain.

Exemple:

Des caméras sont installées à l'entrée d'un bâtiment pour filmer les personnes qui entrent et qui sortent. Leur champ couvre également quelques mètres carrés de la voie publique adjacente, et les caméras filment donc des passants dans une rue fréquentée. Cette pratique est permissible. Il faut par contre éviter de filmer les fenêtres d'un immeuble à appartements situé de l'autre côté de la rue. Il convient dans ce cas de modifier l'emplacement ou l'orientation des caméras, de masquer ou de brouiller les images ou de prendre d'autres mesures similaires.

Dans tous les cas où la surveillance dépasse les points d'entrée et de sortie, il y a lieu d'effectuer une analyse d'impact. Cette surveillance supplémentaire n'est autorisée que pour satisfaire un besoin de sécurité démontré, et moyennant des garanties supplémentaires. Ces garanties peuvent inclure, entre autres, les mesures suivantes:

- restreindre la surveillance des espaces *privés* adjacents (par ex. en masquant ou en brouillant les images);
- dans la mesure du possible, limiter la période de conservation des images à 48 heures (ou pratiquer la surveillance en direct uniquement, sans enregistrement);
- limiter les capacités de zoom des caméras ou la résolution des caméras qui couvrent les espaces publics avoisinants;
- dans la mesure du possible, limiter la surveillance aux moments qui nécessitent une sécurité accrue (par ex. les sommets internationaux ou autres événements spéciaux); et
- donner une formation adéquate aux opérateurs du système de vidéosurveillance pour éviter toute ingérence disproportionnée dans la vie privée des passants ou des autres personnes filmées par les caméras.

L'avis des autorités nationales (ou régionales) de protection des données, des autres pouvoirs compétents et des parties prenantes doit également être pris en considération.

Dans tous les cas, il est important de garder à l'esprit que l'objectif de la vidéosurveillance n'est généralement pas de prévenir la criminalité ni de maintenir l'ordre sur le territoire d'un État membre. Ce rôle revient exclusivement à certains pouvoirs publics des États membres, moyennant le respect des garanties adéquates prévues par la législation nationale. Il se peut, par exemple, que les collectivités locales et/ou les forces de police locales soient les seuls pouvoirs habilités à utiliser ce genre de systèmes. De façon générale donc, aucune institution ne peut légitimement concevoir et installer des systèmes de vidéosurveillance dans ce but.

Cela ne veut pas dire pour autant qu'une institution ne peut pas utiliser son système de vidéosurveillance à cette fin en collaboration avec la police locale (et/ou les autorités locales, le cas échéant) et dans le respect de la législation nationale en vigueur. Dans ce cas, le CEPD recommande de conclure un accord écrit sur ce point. Tout projet de vidéosurveillance de ce type doit faire l'objet d'une analyse d'impact par l'institution concernée.

Exemple:

Dans un pays (hypothétique) où se situe votre bâtiment, la vidéosurveillance des espaces publics tels que les parcs publics et les rues ne peut être pratiquée que par la police locale avec l'accord préalable des autorités locales. Vous recevez à plusieurs reprises des plaintes de membres du personnel de votre institution qui, en rentrant chez eux tard le soir, ont été victimes d'agressions dans le petit parc situé juste devant votre bâtiment. Vous ne pouvez pas, de votre propre initiative, installer des caméras pointées sur le parc pour dissuader les agresseurs. Si la législation locale le permet par contre, vous pouvez coopérer avec la police locale et, moyennant l'accord préalable du gouvernement local, vous pouvez installer et exploiter des caméras pour, par exemple, surveiller l'allée principale du parc entre le crépuscule et l'aube. Il convient également de consulter l'autorité nationale de protection des données pour savoir si vous devez prendre des mesures supplémentaires de protection des données.

Dans les cas où une notification de contrôle préalable est requise, la Commission doit soumettre une seule notification de contrôle préalable au CEPD au nom de toutes les représentations de la Commission dans les États membres.

6.6 Surveillance dans des pays tiers

Les dispositions énoncées au chapitre 6.5 devraient également s'appliquer, *mutatis mutandis*, aux activités de surveillance en dehors du territoire de l'Union européenne. Étant donné que les risques de sécurité et les règles en matière de protection des données varient considérablement en dehors de l'Union européenne, le CEPD recommande aux délégations de la Commission dans les pays tiers d'évaluer de façon indépendante leurs propres besoins de sécurité et de concevoir leurs systèmes de vidéosurveillance en conséquence. Il leur est également conseillé de collaborer avec les autorités locales dans la mesure du possible et pour autant que cette collaboration ne mette pas en danger leur sécurité.

Dans les cas où une notification de contrôle préalable est requise, la Commission doit soumettre une seule notification de contrôle préalable au CEPD au nom de toutes les délégations de l'Union européenne dans les pays tiers.

6.7 Catégories spéciales de données

Les systèmes de vidéosurveillance ne doivent pas avoir pour objectif de saisir (par exemple en zoomant ou en ciblant spécifiquement) ou de traiter (indexation, profilage...) des images révélant des «catégories spéciales de données»: l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé ou à la vie sexuelle[30].

[30] Voir l'article 10 du règlement.

Il convient d'éviter la surveillance d'endroits où les caméras sont susceptibles d'enregistrer des images révélant des catégories spéciales de données, même si l'objectif poursuivi n'est pas de collecter ces catégories spéciales de données[31].

Exemples:

Vous devez éviter de filmer des manifestants ou les salles d'attente du service médical, ou d'installer un système de vidéosurveillance permettant d'enregistrer incidemment des salles d'attentes ou des endroits où protestent des manifestants. Évitez également d'installer des caméras à l'entrée du bureau d'un syndicat ou de surveiller les alentours d'un établissement religieux à l'extérieur de votre bâtiment.

Une analyse d'impact doit être réalisée dans les cas où une institution souhaite déroger à ces règles. La surveillance n'est autorisée que moyennant des garanties supplémentaires.

Dans les cas où la surveillance a pour but d'assurer la sécurité lors de manifestations, ces garanties peuvent, par exemple, comporter les mesures suivantes:

- une manifestation pacifique ne peut faire l'objet d'une surveillance que pour des besoins démontrés de sécurité;
- les caméras ne doivent 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);
- si aucun incident de sécurité n'est détecté, les enregistrements de manifestations pacifiques doivent être effacés dans les 2 heures suivant la fin de la manifestation (une surveillance sans enregistrement peut également être envisagée);
- les images ne peuvent pas servir à des fins d'exploration de données; et
- les opérateurs du système de vidéosurveillance doivent bénéficier d'une formation adéquate pour éviter tout impact disproportionné sur le respect de la vie privée et d'autres droits fondamentaux des participants filmés, y compris, et c'est essentiel, de leur liberté d'association.

Toute surveillance impliquant le traitement de catégories spéciales de données fait l'objet d'un contrôle préalable par le CEPD.

[31] Dans des circonstances ordinaires (par ex. lorsqu'une institution surveille les entrées et sorties de ses bâtiments), le simple fait que le visage ou la silhouette d'une personne, ou encore les vêtements ou les accessoires qu'elle porte, puissent révéler son origine raciale ou ethnique, et peut-être son état de santé, ne signifie pas que l'activité de vidéosurveillance implique le traitement de catégories spéciales de données.

6.8 Sites où les personnes s'attendent à un respect plus important de leur vie privée

Les endroits où les personnes s'attendent à un respect plus important de leur vie privée ne doivent pas faire l'objet d'une surveillance. Il s'agit généralement de bureaux individuels (y compris les bureaux partagés par deux personnes ou plus et des grands bureaux paysagers avec parois de séparation), des endroits de détente (cantines, cafétérias, bars, kitchenettes, salles de repas, salons, salles d'attente, etc.), des sanitaires, des salles de douche et des vestiaires.

Une analyse d'impact doit être réalisée dans les cas où l'institution concernée souhaite déroger à ces règles. Un contrôle préalable par le CEPD est également requis.

6.9 Vidéosurveillance de haute technologie et/ou intelligente

L'utilisation d'outils de vidéosurveillance «de haute technologie» ou de systèmes de vidéosurveillance «intelligents» n'est autorisée que moyennant la réalisation d'une analyse d'impact. L'utilisation de ces systèmes est également soumise à un contrôle préalable. Le CEPD évalue au cas par cas la légitimité de la technologie utilisée et peut, si nécessaire, imposer des garanties supplémentaires en matière de protection des données.

Les outils appartenant à cette catégorie sont notamment:

- la mise en relation du système de vidéosurveillance avec des données biométriques (par ex. des empreintes digitales pour le contrôle d'accès) ou avec toute autre base de données, biométriques ou non (par ex. une base de données de photographies de suspects à des fins de reconnaissance faciale, ou de numéros d'immatriculation pour la reconnaissance de plaques minéralogiques);
- l'indexation des images à des fins de recherches automatiques et d'alertes (par ex. pour suivre des personnes);
- les systèmes de reconnaissance faciale, les autres systèmes de reconnaissance d'images ou les systèmes de reconnaissance de démarche;
- toute forme de surveillance dynamique-préventive (par ex. les logiciels d'analyse automatique des comportements permettant de déclencher des alertes automatiques sur la base de comportements suspects prédéfinis ou de certains mouvements, styles de vêtements ou langages corporels);
- un réseau de caméras doté d'un logiciel de suivi capable de suivre des objets ou des personnes en mouvement à travers toute la zone couverte par le réseau;
- les systèmes d'alerte basés sur des signaux acoustiques (déclenchés par une modification du bruit, par exemple un cri soudain);
- les caméras infrarouges ou quasi-infrarouges, les dispositifs d'imagerie thermique et autres caméras spéciales capables de filmer dans l'obscurité ou la pénombre, de voir à travers les murs ou sous les vêtements (par ex. les scanners corporels); et
- les caméras spécialisées dotées de zooms optiques et numériques améliorés.

Les dispositifs suivants, par contre, ne nécessitent pas automatiquement une analyse d'impact ou un contrôle préalable:

- les détecteurs de mouvement permettant de limiter les prises de vues aux événements méritant d'être observés et enregistrés;
- la configuration d'un système de détection de mouvements capable d'alerter le personnel de sécurité lorsqu'il détecte l'accès à une zone restreinte (par ex. une salle informatique verrouillée en dehors des heures de bureau);
- les capacités habituelles de balayage horizontal et vertical et les zooms optiques et numériques de puissance limitée.

En cas de doute quant à la nécessité d'un contrôle préalable, veuillez nous contacter.

6.10 Interconnexion de systèmes de vidéosurveillance

L'interconnexion du système de vidéosurveillance d'une institution avec le système de vidéosurveillance d'une autre institution ou de toute autre partie tierce doit faire l'objet d'une analyse d'impact. Une analyse d'impact est requise également dans les cas où une même institution utilise plusieurs systèmes distincts (par exemple dans différentes villes, ou différents systèmes sur le même site mais servant des finalités différentes) et souhaite les interconnecter. Une notification de contrôle préalable est également requise.

6.11 Surveillance dissimulée

Aux fins des présentes lignes directrices, on entend par «surveillance dissimulée» les systèmes de surveillance dont les caméras sont

- dissimulées intentionnellement; ou
- installées sans que le public en soit correctement informé, ce qui fait que l'on peut raisonnablement supposer que les personnes surveillées n'ont pas conscience de leur présence.

Si des caméras sont installée dans des endroits où les personnes s'attendent à un plus grand respect de leur vie privée (voir le chapitre 6.8), sans respecter simultanément les deux conditions ci-dessous, la vidéosurveillance sera considérée comme dissimulée même si un avis général à l'entrée du bâtiment signal que le bâtiment fait l'objet d'une vidéosurveillance:

- un avis spécifique et clairement visible est affiché à l'endroit précis concerné (par exemple sur la porte d'un bureau personnel); et
- une politique de vidéosurveillance publiquement disponible rédigée conformément aux recommandations du chapitre 11 fournit des explications spécifiques quant à la possibilité de surveillance dans ces endroits (par ex. les bureaux individuels).

.

Du fait de son caractère secret, la surveillance dissimulée est hautement intrusive.

Par ailleurs, elle n'a guère d'effet préventif et n'est souvent envisagée que comme un piège permettant de rassembler des preuves. Il convient donc d'éviter d'y avoir recours.

Les propositions d'exception à ce principe doivent être assorties d'une justification convaincante, d'une analyse d'impact, et doivent faire l'objet d'un contrôle préalable par le CEPD. Si nécessaire, celui-ci peut proposer des mesures spécifiques pour garantir la protection des données.

En principe, il est peu probable que le CEPD rende un avis de contrôle préalable positif si toutes les conditions suivantes ne sont pas respectées:

- la surveillance dissimulée est envisagée dans le but d'enquêter sur un délit suffisamment grave dans le cadre d'une enquête formelle, exigée ou autorisée par la loi et menée par la police d'un État membre, par d'autres agents compétents des forces de l'ordre ou par les organes d'enquête compétents de l'UE;
- le recours à la surveillance dissimulée est conforme à la loi et a été autorisé formellement (i) par un juge ou un autre magistrat habilité à le faire en vertu des lois de l'État membre qui a demandé le recours à la surveillance dissimulée au sein de l'institution; ou (ii) par l'organe décisionnel supérieur compétent de l'institution conformément au règlement écrit et publiquement disponible de l'institution concernant le recours à la surveillance dissimulée (par ex. un comité exécutif supérieur);
- l'institution tient un registre de toutes les autorisations de ce type et de tous les recours à la surveillance dissimulée et ce registre doit être mis à la disposition du DPD et du CEPD sur demande;
- les caméras sont installées pour une période strictement limitée et dans des endroits bien précis;
- il n'existe aucune alternative à l'utilisation de la surveillance dissimulée pour enquêter avec succès sur l'affaire concernée; et
- les bénéfices escomptés compensent la violation de la vie privée des personnes concernées.

6.12 Enregistrement sonore et «caméra de surveillance parlante»[32]

Du fait de leur caractère intrusif, l'utilisation d'enregistrements sonores et de «caméras de surveillance parlantes» est également interdite en principe, sauf en guise de système de secours pour le contrôle d'accès en dehors des heures de bureau (en tant que visiophone pour contacter le personnel de sécurité à distance afin d'obtenir un accès).

Lorsque ce système est utilisé comme système de secours pour le contrôle d'accès,

[32] Aux fins des présentes lignes directrices, on entend par «caméra de surveillance parlante» tout système de vidéosurveillance utilisant des haut-parleurs installés à l'endroit de la surveillance et permettant aux opérateurs du système de «s'adresser» aux personnes sous surveillance (par ex. «le monsieur à la veste en cuir marron, veuillez ramasser les déchets que vous venez de jeter par terre...»).

cette utilisation doit être clairement indiquée et les caméras peuvent diffuser ou enregistrer du son uniquement (i) lorsque cette fonctionnalité est activée personnellement par la personne qui cherche à accéder aux locaux; ou (ii) après un certain nombre de tentatives d'accès infructueuses.

Toute autre proposition d'exception doit être accompagnée d'une justification convaincante, d'une analyse d'impact et faire l'objet d'un contrôle préalable.

7 Durée de conservation des enregistrements

7.1 Période de conservation

7.1.1 Principes généraux. Les enregistrements ne doivent pas être conservés plus longtemps que nécessaire pour atteindre l'objectif pour lequel ils ont été réalisés[33]. Il convient également de se demander si l'enregistrement est effectivement nécessaire, ou si une surveillance en direct sans enregistrement serait suffisante.

Si l'institution opte pour l'enregistrement, elle doit préciser la durée de conservation des enregistrements. Une fois cette durée écoulée, les enregistrements doivent être effacés. Il est recommandé d'automatiser si possible le processus d'effacement, par exemple, en réutilisant automatiquement et périodiquement les supports selon le principe «first in, first out». Lorsqu'un support est devenu inutilisable (après un certain nombre de cycles), il doit être éliminé de façon à ce que les données restantes soient supprimées de façon permanente et irréversible (par exemple par broyage ou par un traitement équivalent).

Si la vidéosurveillance est utilisée à des fins de sécurité et de contrôle d'accès, et si un incident de sécurité se produit et qu'il est établi que les enregistrements sont nécessaires pour enquêter sur cet incident, ou si ces enregistrement doivent servir de preuves, les passages concernés peuvent être conservés au-delà de la période de conservation normale et aussi longtemps que nécessaire. Une fois le dossier clôturé, ils doivent également être effacés.

Exemple:

Une agence utilise un système de vidéosurveillance à des fins de sécurité et de contrôle d'accès. L'agence doit préciser un délai, par exemple 3 jours calendrier, au terme duquel les enregistrements sont automatiquement écrasés.

Si un incident de sécurité est détecté au cours de ces trois jours, par exemple si un incendie se déclare dans le garage du bâtiment, les passages concernés peuvent être conservés pour toute la durée de l'enquête menée à propos de cet incident.

7.1.2 Période de conservation pour une utilisation typique à des fins de

[33] Règlement, article 4, paragraphe 1, point e).

sécurité: une semaine. Lorsque les caméras sont installées à des fins de sécurité et de contrôle d'accès, un délai d'une semaine est en général largement suffisant pour permettre au personnel de sécurité de prendre une décision informée quant à la nécessité de conserver éventuellement certains passages plus longtemps pour les besoins d'une enquête ou pour servir de preuves. À vrai dire, ces décisions peuvent généralement être prises en quelques heures. Les institutions doivent donc définir une période de conservation ne dépassant pas sept jours calendrier[34]. Dans la plupart des cas, une période plus courte devrait suffire.

7.1.3 Territoire d'un État membre ou d'un pays tiers: 48 heures. Si la surveillance couvre un espace situé en dehors des bâtiments sur le territoire d'un État membre ou d'un pays tiers (généralement à proximité des entrées et sorties) et s'il n'est pas possible d'éviter d'avoir des passants ou des véhicules dans le champ de vision des caméras, le CEPD recommande de réduire la période de conservation à 48 heures ou de tenir compte le plus possible des préoccupations locales.

Exemple:

Les agences A et B utilisent toutes deux un système de vidéosurveillance à des fins de sécurité et de contrôle d'accès.

L'agence A est installée dans une zone rurale éloignée, avec très peu de circulation de piétons ou de véhicules à proximité. Ses locaux sont entourés d'une clôture donnant sur les champs. L'agence A peut conserver ses enregistrements pendant plus de 48 heures (mais pas plus de sept jours calendrier). Par exemple, elle peut décider d'adopter la même période de conservation de 3 jours pour la surveillance de ses locaux et celle du voisinage immédiat de ses locaux.

L'agence B est installée au cœur d'un centre-ville animé, à proximité d'une gare, avec une circulation piétonne importante sur le trottoir au pied de ses bâtiments. L'agence B doit faire en sorte que la durée de conservation des enregistrements couvrant l'extérieur de ses bâtiments soit limitée à 48 heures au plus. Elle devrait également envisager la possibilité d'une durée de conservation plus courte ou d'un mode de surveillance sans enregistrement.

7.1.4 Périodes de conservation plus courtes. Le CEPD peut recommander des périodes de conservation plus courtes ou une surveillance en direct uniquement dans les cas où cette mesure est nécessaire pour réduire au minimum l'impact sur le respect de la vie privée et d'autres droits fondamentaux et intérêts légitimes des personnes passant dans le champ de vision des caméras.

[34] Voir l'avis 4/2004 du groupe de travail «Article 29» sur la protection des données concernant le traitement de données à caractère personnel au moyen de la vidéosurveillance, partie 7(E), page 20.

Exemple:

Des manifestations politiques sont organisées régulièrement devant vos bâtiments. Vous soumettez votre contrôle préalable au motif que des catégories spéciales de données sont susceptibles d'être traitées (voir chapitre 6.7). Considérant les circonstances, le CEPD peut recommander, si aucun incident de sécurité n'est détecté, d'effacer les enregistrements de chaque manifestation pacifique dans les 2 heures suivant la fin de la manifestation (ou d'envisager une surveillance en direct sans enregistrement).

7.2 Registre des enregistrements conservés au-delà du délai normal

L'institution doit tenir un registre - si possible sous forme électronique - de tous les enregistrements conservés au-delà de la période de conservation normale. Ce registre doit indiquer:

- la date et l'heure de la séquence et l'emplacement de la caméra;
- une brève description de l'incident de sécurité;
- la raison pour laquelle la séquence doit être conservée; et
- la date prévue à laquelle la nécessité de conserver cette séquence sera réévaluée.

Exemple d'entrée du registre:

- *Date et heure de la séquence: 1er octobre 2009, entre 10 h 00 et midi*
- *Emplacement caméra: caméra n° 5 (entrée ascenseur dans le parking)*
- *Brève description de l'incident de sécurité: départ de feu dans la poubelle à côté de l'entrée de l'ascenseur dans le parking. Pas de dégâts ni de blessures corporelles.*
- *Raison de conservation de la séquence: l'unité de sécurité a besoin de la séquence de vidéosurveillance dans le cadre de l'enquête afin de déterminer la cause de l'incendie, d'en tirer des apprentissages et de déterminer les mesures de protection à prendre éventuellement.*
- *Date prévue de réexamen de la nécessité de conserver la séquence: 15 octobre 2009.*

8 Personnes autorisées à accéder aux images

8.1 Un petit nombre de personnes clairement identifiées, sur la base du «besoin de savoir»

L'accès au système et aux images doit être réservé à un petit nombre de personnes clairement identifiées, sur la base du «besoin de savoir» Il convient également de faire en sorte que les utilisateurs autorisés puissent uniquement accéder aux

données personnelles correspondant à leurs droits d'accès[35]. Il y a lieu de définir des politiques de contrôle d'accès selon le principe du «privilège minimal»: les utilisateurs doivent avoir accès uniquement aux informations strictement nécessaires pour l'exécution de leur travail.

Seuls le «responsable du traitement», l'administrateur du système ou les autres membres du personnel désignés expressément par le responsable du traitement doivent être habilités à accorder, modifier ou supprimer des droits d'accès. L'octroi, la modification et la suppression de droits d'accès doivent toujours se faire dans le respect des critères définis par la politique de vidéosurveillance de l'institution.

Les utilisateurs possédant des droits d'accès doivent être des personnes clairement identifiables à tout moment.

Exemple:

Il faut éviter d'attribuer un nom d'utilisateur ou mot de passe commun à une société de sécurité externe employant plusieurs personnes au sein de votre institution.

La politique de vidéosurveillance doit spécifier et documenter clairement qui a accès aux séquences de vidéosurveillance et/ou à l'architecture technique du système de vidéosurveillance, la raison de cet accès et la nature précise des droits d'accès. Il y a notamment lieu de spécifier qui a le droit:

- de visionner les séquences en temps réel;
- de commander les caméras à balayage horizontal, vertical et zoom (*pan/tilt/zoom*, PTZ);
- de visionner les séquences enregistrées; ou
- de copier,
- télécharger,
- supprimer ou
- modifier une séquence.

Toute différence entre les droits accordés à différentes catégories de personnes doit être spécifiée clairement.

Par exemple, les personnes

- qui contrôlent les images en direct,
- qui sont responsables de la maintenance technique du système ou
- qui enquêtent sur les incidents de sécurité

ont différentes tâches et devraient donc avoir différents droits d'accès au système.

[35] Sur ce dernier point, voir l'article 22, paragraphe 2, point e) du règlement.

Le personnel interne et les sous-traitants extérieurs ont également différentes tâches et doivent donc posséder des droits d'accès différents.

Les droits d'accès doivent être pris en compte au niveau technique par le système. Par exemple, le profil d'utilisateur d'une personne peut lui permettre de copier des séquences enregistrées tandis que le profil d'une autre personne lui permettra seulement de les visionner.

Par ailleurs, la politique d'accès doit décrire clairement les conditions dans lesquelles les droits d'accès peuvent être exercés, par exemple les cas dans lesquels une personne dont le profil permet la copie ou la suppression est effectivement autorisée à copier ou à supprimer une séquence.

Dans le cas d'une vidéosurveillance pratiquée à des fins de sécurité et de contrôle d'accès, les droits d'accès doivent être limités exclusivement au personnel de sécurité interne ou externe (sous-traitants) et au personnel chargé de la maintenance technique du système.

Exemple:

Les gardiens de sécurité employés par une société externe et travaillant dans votre salle de contrôle peuvent avoir le droit de visionner les images en temps réel, de commander les caméras PTZ (par exemple pour zoomer sur un objet) ou de visionner des séquences enregistrées en ligne, mais ils ne devraient pas avoir la possibilité technique de copier, de télécharger, de supprimer ou de modifier une séquence.

En outre, si les gardiens sont chargés de contrôler les images en temps réel et de commander les caméras PTZ en fonction des besoins de leur mission de surveillance, ils doivent recevoir pour consigne de ne pas utiliser les caméras PTZ pour zoomer sur une cible, par exemple un groupe de personnes qui manifestent pacifiquement en face du bâtiment ou deux membres du personnel qui passent dans le champ de la caméra, si cette action n'est pas nécessaire pour atteindre les objectifs de sécurité et de contrôle d'accès pour lesquels la surveillance est pratiquée.

8.2 Formation à la protection des données

Tous les membres du personnel possédant un droit d'accès, y compris le personnel extérieur chargé des opérations de vidéosurveillance au quotidien ou de la maintenance du système, doivent recevoir une formation à la protection des données et se familiariser avec les dispositions des présentes lignes directrices dans la mesure où celles-ci sont pertinentes pour leur travail. Cette formation doit accorder une attention particulière à la nécessité d'empêcher la divulgation de séquences de vidéosurveillance à toute personne non autorisée.

Une formation doit être organisée lors de l'installation d'un nouveau système, en cas de modifications importantes apportées à un système existant, lors de la prise de

fonctions d'une nouvelle personne ainsi qu'à intervalles réguliers par la suite. Pour les systèmes existants, une formation initiale doit être organisée au cours de la période transitoire, avant le 1er janvier 2011.

8.3 Confidentialité

Tous les membres du personnel possédant un droit d'accès, y compris le personnel extérieur chargé des opérations de vidéosurveillance au quotidien ou de la maintenance du système, de même que les sociétés extérieures elles-mêmes, doivent signer un accord de confidentialité les engageant à ne pas transférer, montrer ou divulguer de quelque façon que ce soit le contenu de toute séquence de vidéosurveillance à une personne autre que les destinataires autorisés.

9 Mesures de sécurité à prendre pour protéger les données[36]

Avant tout, il y a lieu d'effectuer une analyse interne des risques de sécurité afin de déterminer les mesures de sécurité nécessaires pour protéger le système de vidéosurveillance, y compris les données à caractère personnel qu'il traite.

Dans tous les cas, des mesures doivent être prises pour garantir la sécurité en matière

- de transmission;
- de stockage (par ex, dans des bases de données informatiques); et
- d'accès (par ex. accès aux systèmes informatiques et aux locaux).

La transmission doit passer par des moyens de communication sécurisés et protégés contre l'interception. La protection contre l'interception est particulièrement importante en cas d'utilisation d'un système de transmission sans fil ou de transfert de séquences via l'internet. Dans de tels cas, les données doivent être cryptées pendant leur transmission ou bénéficier d'une protection équivalente.

Le cryptage ou d'autres moyens techniques offrant une protection équivalente doivent également être envisagés dans d'autres cas, au niveau de la transmission ou du stockage, si l'analyse interne des risques de sécurité le justifie, par exemple dans le cas de séquences particulièrement sensibles.

Tous les locaux servant au stockage ou au visionnage de séquences de vidéosurveillance doivent être sécurisés. L'accès physique à la salle de contrôle et à la salle de stockage des séquences de vidéosurveillance doit être protégé. Aucune partie tierce (par ex. personnel d'entretien ou de maintenance) ne doit pouvoir accéder à ces locaux sans surveillance.

L'emplacement des moniteurs doit être défini de façon à ce que les images ne soient pas visibles pour le personnel non autorisé. S'ils doivent être placés près de la réception, les moniteurs doivent être orientés de façon à ce que seul le personnel de

[36] Voir l'article 22 du règlement.

sécurité puisse les consulter.

Un système d'archivage numérique fiable doit être mise en place pour permettre, en cas d'audit, de déterminer à tout moment qui a accédé au système, où et quand. Le système d'archivage doit être en mesure d'identifier qui a visionné, supprimé, copié ou modifié n'importe quelle séquence de vidéosurveillance. À cet égard comme ailleurs, il convient d'accorder une attention particulière aux rôles et aux pouvoirs essentiels des administrateurs du système et à la nécessité de compenser ces pouvoirs par des mesures de contrôle et de protection suffisantes.

Une procédure doit également être définie pour réagir de façon adéquate à toute divulgation involontaire d'informations personnelles. Cette procédure doit prévoir, dans la mesure du possible, le signalement de la faille de sécurité aux personnes dont les données ont été divulguées par inadvertance ainsi qu'au DPD de l'institution.

L'analyse de sécurité et les mesures prises pour protéger les séquences de vidéosurveillance doivent être correctement documentées et doivent être mises à la disposition du CEPD sur demande.

Enfin, l'institution doit faire preuve d'une diligence raisonnable dans le choix et le contrôle du personnel extérieur.

10 Transferts et divulgations

10.1 Cadre général

Le règlement comporte trois règles principales régissant les transferts, selon que les enregistrements sont transférés (i) à un destinataire au sein de l'institution ou dans une autre institution; (ii) à d'autres destinataires à l'intérieur de l'Union européenne; ou (ii) à l'extérieur de l'Union européenne[37].

Dans le premier cas, le règlement prévoit que les enregistrements peuvent faire l'objet d'un transfert au sein de l'institution ou vers une autre institution si ce transfert est nécessaire à l'exécution légitime de missions relevant de la compétence du destinataire. (Voir le chapitre 10.3 pour plus de détails et des exemples.)

Dans le deuxième cas (transfert en dehors des institutions mais à l'intérieur de l'Union européenne), ce transfert est possible s'il est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique, ou si le destinataire démontre la nécessité du transfert et s'il n'existe aucune raison de penser que ce transfert pourrait porter atteinte aux intérêts légitimes des personnes dont les images sont transférées. (Voir le chapitre 10.4 pour plus de détails et des exemples.)

[37] Les transferts sont possibles en vertu des articles 7, 8 ou 9 du règlement. Ces articles doivent être lus conjointement avec d'autres dispositions du règlement, et notamment les articles 4, 5, 6 et 10. En outre, les enregistrements peuvent également être remis aux personnes concernées conformément à leur droit d'accès visé à l'article 13 du règlement (voir le chapitre 12 des lignes directrices).

Troisièmement, un transfert vers l'extérieur de l'Union européenne est possible (i) s'il a pour seul objectif de permettre l'exécution de la mission de l'institution[38] et (ii) moyennant le respect de conditions supplémentaires visant principalement à garantir la protection adéquate des données à l'étranger. (Voir le chapitre 10.4 pour plus de détails et des exemples.)

Pour évaluer la légalité du transfert, il convient toutefois de prendre en considération de nombreuses autres dispositions du règlement qui définissent d'autres conditions à respecter pour pouvoir procéder au transfert. Il est important de souligner que dans la plupart des cas, aucun transfert ne peut être effectué à des fins incompatibles avec l'objectif initialement défini du système de vidéosurveillance.

Exemple:

Si le système de vidéosurveillance est installé à des fins de sécurité, et s'il a été annoncé comme tel, les enregistrements ne peuvent pas êtres communiqués par la suite au supérieur d'un membre du personnel qui en fait la demande en vue de prouver que l'employé en question est arrivé en retard au travail.

Il existe un petit nombre d'exceptions importantes à cette règle[39]. La plus importante de ces exceptions concerne les demandes de transfert émanant de la police à des fins d'enquête ou de poursuites de délits (voir le chapitre 10.4).

10.2 Transferts *ad hoc* et systématiques

La décision d'autoriser ou non un transfert nécessite souvent de trouver un équilibre délicat entre les droits de la personne et les droits ou les intérêts de ceux qui demandent la séquence vidéo. Chaque transfert doit être soigneusement évalué au cas par cas.

Dans tous les cas de transfert *ad hoc*, il convient également de demander systématiquement l'avis du DPD quant à la légalité du transfert conformément au règlement. En cas de transferts récurrents et similaires, l'évaluation en matière de protection des données peut toutefois aussi être similaire. Ces transferts typiques doivent être décrits dans la politique de vidéosurveillance de l'institution. Une fois qu'une politique concernant ces transferts a été définie, il n'est plus nécessaire de consulter le DPD à propos de chaque transfert de routine, même s'il est toujours recommandé de le faire en cas de doute.

[38] Il existe certaines exceptions à cette règle en vertu de l'article 9, paragraphe 6, qui stipule notamment qu'un transfert peut être nécessaire pour «la constatation d'un droit en justice». Cette disposition doit être interprétée comme couvrant les demandes introduites par la police dans le contexte d'une enquête pénale.

[39] Voir l'article 20 du règlement.

Exemple:

Les caméras installées à proximité de votre entrée principale couvrent également le parking pour vélos voisin. Tous les quelques mois, la police locale demande le transfert des enregistrements concernés pour l'aider dans la lutte contre les vols de vélos. Vous devez posséder une politique indiquant la suite à donner à ces demandes. Une fois ces règles en place, il ne sera pas nécessaire de consulter à chaque fois votre DPD.

10.3 Transferts aux organes d'enquête de l'UE

Moyennant l'analyse au cas par cas décrite ci-dessus, et compte tenu de la finalité initiale de l'enregistrement, les séquences concernées (par exemples les séquences susceptibles de constituer des preuves) peuvent être transférées dans des cas exceptionnels si les organes suivants en font la demande:

- l'Office européen de lutte antifraude (**OLAF**), dans le cadre d'une enquête menée par l'OLAF;
- 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
- les organes chargés de mener une enquête interne ou une procédure disciplinaire au sein de votre institution.

Ces transferts sont acceptables s'il y 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*) doivent être rejetées.

La direction, le service des ressources humaines ou les autres personnes impliquées ne doivent pas recevoir de copies ni bénéficier d'un accès aux séquences de vidéosurveillance en dehors des procédures formelles décrites ci-dessus. En cas de doute, il convient de consulter en premier lieu le DPD.

Exemple:

Un employé porte plainte pour harcèlement moral contre son supérieur direct, qui lance à son tour une procédure pour incompétence professionnelle contre son employé. En dehors du cadre de ces procédures, le supérieur vous demande informellement d'«ouvrir l'œil» pour identifier d'éventuelles images suspectes de l'employé, par exemple des passages au bureau en dehors des heures de travail, des arrivées tardives ou la visite sans surveillance des bureaux d'autres personnes. Vous ne devez en aucun cas accéder à des demandes de ce genre.

Enfin, des séquences de vidéosurveillance peuvent également être communiquées au CEPD, par exemple lorsque le CEPD effectue une inspection sur place ou mène une enquête à la suite d'une plainte.

10.4 Transferts aux autorités nationales

Moyennant l'analyse au cas par cas décrite ci-dessus, et compte tenu de la finalité initiale de l'enregistrement, il est possible dans certains cas de communiquer des séquences de vidéosurveillance à la police nationale, aux tribunaux ou à d'autres autorités nationales.

Si la police, un tribunal ou d'autres autorités nationales demandent la divulgation d'enregistrements, l'institution doit insister pour recevoir une demande écrite respectant les obligations de forme et de contenu imposées par la législation nationale en vigueur. L'institution ne doit divulguer ces enregistrements que dans les cas où une autre institution installée dans ce pays, dans des circonstances similaires, aurait été obligée ou au moins autorisée à les divulguer.

Chaque fois que possible et indépendamment des obligations imposées au niveau national, l'institution doit demander un mandat judiciaire, une demande écrite signée par un officier de police suffisamment gradé ou une demande formelle similaire. Cette demande devrait aussi spécifier, le plus précisément possible, la raison pour laquelle la séquence de vidéosurveillance est nécessaire ainsi que l'endroit, la date et l'heure de la séquence demandée.

Dans la plupart des cas, l'institution peut accéder aux demandes de la police nationale lorsque les enregistrements sont nécessaires dans le cadre d'une enquête ou de poursuites concernant des délits, pour autant que la demande s'inscrive dans le cadre d'une enquête spécifique. Les demandes générales en vue d'une exploration des données (*data mining*) doivent par contre être rejetées.

Exemple:

Une manifestation est organisée devant votre bâtiment pour réclamer la régularisation de la situation des immigrants sans papiers, dont certains y participent. À la fin de cette manifestation, qui s'est déroulée de façon pacifique et sans incidents, la police nationale vous demande de lui remettre toutes les séquences de vidéosurveillance enregistrées sans faire référence à une enquête particulière, dans l'intention d'utiliser les images pour identifier les immigrés en situation irrégulière et de conserver ces images pour les utiliser ultérieurement en cas de besoin. Vous ne devez en aucun cas accéder à une demande de ce genre.

On notera également que si la police ou une autre organisation nationale d'un État membre introduit une demande d'accès dans le cadre d'une procédure officielle, elle devra d'abord obtenir une levée d'immunité si la séquence en question concerne un membre du personnel d'une institution de l'Union.

10.5 Registre des transferts et divulgations

Les institutions doivent tenir un registre des transferts et divulgations, si possible au format électronique. Chaque transfert à une partie tierce doit y être noté. (Les «parties tierces» incluent également les autres membres de l'institution recevant un enregistrement des personnes qui y ont accès à l'origine. Ces transferts incluent généralement tous les transferts vers l'extérieur de l'unité de sécurité.) Ce registre devrait également noter tous les cas où, même si aucune copie de séquence n'a été transférée, des parties tierces ont pu visionner des enregistrements, ou encore les cas où le contenu de certains enregistrements a été communiqué à des parties tierces.

Ce registre doit comprendre au minimum les données suivantes:

- la date des enregistrements;
- la partie ayant introduit la demande (nom, titre, organisation);
- le nom et le titre de la personne ayant autorisé le transfert;
- une description succincte du contenu des enregistrements;
- la raison de la demande et la raison pour laquelle cette demande a été approuvée; et enfin,
- une précision indiquant si la séquence a été transférée, si elle a été montrée ou si des informations ont été données verbalement.

Le DPD et le CEPD peuvent demander à tout moment à l'institution de leur remettre une copie du registre à des fins d'examen.

11 Comment communiquer des informations au public

11.1 Approche à plusieurs niveaux

Les informations relatives à la vidéosurveillance doivent être communiquées au public de façon complète et effective[40]. Les présentes lignes directrices recommandent une approche à plusieurs niveaux associant les deux méthodes suivantes:

- des avis affichés sur place permettant d'informer directement le public de la vidéosurveillance et de lui fournir les informations essentielles relatives au traitement; et
- un avis détaillé de protection des données publié sur l'intranet et le site internet de l'institution pour ceux qui souhaitent en savoir plus. Afin d'éviter une duplication des efforts, l'institution peut publier en ligne la version publique de sa politique de vidéosurveillance plutôt que de rédiger un avis distinct en matière de protection des données.

[40] Pour la liste des informations que la législation impose de fournir dans votre avis, voir l'article 12 du règlement.

Ces deux méthodes peuvent être complétées par d'autres encore. Par exemple, des exemplaires imprimés de l'avis relatif à la protection des données doivent être disponibles auprès de la réception et de l'unité de sécurité sur demande, et l'institution doit également communiquer un numéro de téléphone et une adresse électronique pour les demandes d'informations supplémentaires. La disponibilité d'informations plus détaillées sur l'intranet, l'internet (et sous la forme de brochures ou par d'autres moyens encore)) ne dispense toutefois pas d'afficher des avis sur place.

11.2 Avis sur place

Les avis affichés sur place doivent inclure un pictogramme (par exemple le pictogramme ISO ou le pictogramme utilisé habituellement à l'endroit où se situe le bâtiment) et une partie des informations visées à l'article 12 du règlement - le maximum raisonnable d'informations selon les circonstances. Cet avis doit:

- identifier le «responsable du traitement» (le nom de l'institution est généralement suffisant);
- spécifier la finalité de la surveillance («pour votre sécurité» est généralement suffisant);
- indiquer clairement si les images sont enregistrées;
- fournir des informations de contact et un lien vers la politique de vidéosurveillance disponible en ligne.
- Si la surveillance s'étend à n'importe quel endroit en dehors du bâtiment, l'avis doit le préciser clairement. Dans un tel cas, un avis indiquant simplement que *le bâtiment* fait l'objet d'une vidéosurveillance prête à confusion.

Le personnel de sécurité et l'équipe de réception doit avoir reçu une formation relative aux aspects de protection des données de la vidéosurveillance et être en mesure de distribuer immédiatement des copies de l'avis détaillé en matière de protection des données (politique de vidéosurveillance) sur simple demande. Ces employés doivent également pouvoir donner aux membres du public le nom de la personne à contacter pour toute question supplémentaire ou pour avoir accès aux données les concernant.

Ces avis doivent être placés aux endroits opportuns et avoir un format suffisant pour que les personnes concernées puissent les remarquer avant de pénétrer dans la zone surveillée et qu'elles puissent les lire sans difficulté. Cela ne signifie pas pour autant qu'il faille afficher un avis à côté de chaque caméra.

Exemple:

Votre institution emploie cinquante personnes et occupe un petit immeuble dans une zone urbaine dense. Il vous est recommandé d'afficher des avis au format A3 à l'entrée principale du bâtiment, une affiche un peu plus grande à l'entrée du parking (de façon à ce que l'avis soit visible depuis le siège du conducteur) ainsi que d'autres avis au format A3 près des accès aux ascenseurs dans le parking et au rez-de-chaussée. S'il existe plusieurs entrées, un avis doit être affiché à chaque entrée.

Les affiches situées à l'intérieur du bâtiment doivent être dans la ou les langue(s) généralement comprises par les membres du personnel et les visiteurs les plus fréquents. Les avis situés à l'extérieur des bâtiments (si la surveillance couvre des espaces extérieurs) doivent également être affichés dans la ou les langue(s) locale(s).

Si des caméras sont installées dans des endroits où les personnes s'attendent à un respect plus important de leur vie privée (voir chapitre 6.8) ou dans des endroits où la présence de caméras est inattendue et donc surprenante, il convient d'afficher un avis supplémentaire à proximité immédiate de la zone surveillée (par exemple sur la porte d'un bureau individuel sous surveillance) [41].

L'annexe 2 fournit un exemple d'avis à afficher sur place, que les institutions peuvent personnaliser selon leurs besoins.

11.3 Politique de vidéosurveillance en ligne

En adoptant une politique de vidéosurveillance et en la publiant sur votre intranet et sur votre site internet, vous respectez également votre obligation de fournir un avis détaillé en matière de protection des données. Il ne sera donc pas nécessaire de rédiger et de publier séparément un avis de protection des données en ligne.

Pour pouvoir servir correctement d'avis en matière de protection des données, votre politique de vidéosurveillance doit contenir les informations suivantes dans un langage et un format facilement lisibles:

- l'identité du responsable du traitement (par exemple l'institution, la direction générale, la direction et l'unité);
- une description succincte de la couverture du système de vidéosurveillance (par ex. entrées et sorties, salles informatiques, salles d'archive);
- la base juridique de la vidéosurveillance;
- les données collectées et la finalité de la vidéosurveillance (toutes les restrictions en matière d'utilisation autorisée doivent également être précisées clairement);
- les personnes qui ont accès aux séquences de vidéosurveillance et celles à qui les images sont susceptibles d'être divulguées;
- la façon dont les informations sont protégées et sauvegardées;
- la durée de conservation des données;
- la procédure à suivre par les personnes concernées pour vérifier, modifier ou supprimer leurs informations (avec des coordonnées permettant d'obtenir de plus amples informations et des informations sur la façon de lancer un recours en interne);
- le droit de saisir le CEPD à tout moment.

[41] Voir également le chapitre 6.11 sur la vs dissimulée.

Par ailleurs, la politique de vidéosurveillance doit également fournir des hyperliens vers:

- les lignes directrices du CEPD en matière de vidéosurveillance;
- les rapports d'audit de l'institution;
- le(s) rapport(s) de l'analyse d'impact de l'institution; et
- le cas échéant, l'avis rendu par le CEPD au terme du contrôle préalable.

L'annexe 1 fournit un modèle de politique de vidéosurveillance (qui peut également servir d'avis en ligne sur la protection des données) pour un système de vidéosurveillance standard. Cette politique peut être adaptée en fonction des circonstances.

11.4 Notification individuelle

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

- l'identité de la personne a été notée dans un dossier/un enregistrement;
- l'enregistrement vidéo est utilisé à l'encontre de la personne;
- l'enregistrement vidéo est conservé au-delà du délai normal;
- l'enregistrement vidéo est transféré à l'extérieur de l'unité de sécurité *ou*
- l'identité de la personne est communiquée à une personne extérieure à l'unité de sécurité;

La notification peut parfois être retardée temporairement, par exemple si ce délai est nécessaire pour l'enquête ou pour la prévention, la détection ou la poursuite de délits[42]. Si une situation de ce type se présente, veuillez demander conseil à votre DPD.

12 Comment répondre aux demandes d'accès de la part du public

Lorsqu'une personne demande quelles données l'institution traite à son sujet, il convient de réagir à cette requête sans retard et avec tous les détails qu'il est raisonnable de fournir pour répondre à ses préoccupations.

S'il s'agit d'une demande générale, il suffit normalement de renvoyer la personne à la politique de vidéosurveillance.

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

Exemple:

Une personne résidant dans l'État membre A, où se situe votre bâtiment, vous envoie le courriel suivant: «Je m'inquiète de la vidéosurveillance pratiquée à l'extérieur de votre bâtiment, devant lequel je passe tous les jours. Je vous serais reconnaissant(e) de me fournir de plus amples informations concernant cette vidéosurveillance et les données qui sont traitées à mon sujet.» Une réponse générale renvoyant ce citoyen/cette citoyenne à votre politique de vidéosurveillance est suffisante.

Les requêtes plus spécifiques nécessitent une réponse plus détaillée. Si la personne en fait expressément la demande, il convient de lui donner accès aux enregistrements - soit en lui permettant de les visionner, soit en lui en remettant une copie. Dans ce cas, il y a lieu de prendre soigneusement en considération les droits des autres personnes visibles sur les mêmes enregistrements, et de les protéger si nécessaire (soit en demandant leur accord pour les divulguer, soit en les masquant ou en brouillant leur image). La protection des droits des parties tierces ne peut toutefois pas servir de prétexte pour rejeter les demandes légitimes, surtout dans les cas où les enregistrements sont utilisés comme preuves.

Exemples:

Un employé faisant l'objet d'une procédure disciplinaire pour harcèlement moral vous demande si vous avez examiné spécifiquement, et communiqué à la direction, à la police ou à d'autres personnes des séquences de vidéosurveillance le concernant dans le cadre de cette procédure. Si tel n'est pas le cas, un simple «non» est une réponse suffisante.

Si par contre vous avez effectivement communiqué certaines séquences à des tiers, vous devez le dire et préciser le contenu des séquences, la date et le lieu de leur enregistrement, la personne à laquelle vous les avez transmises et la raison du transfert.

Si l'employé en fait la demande expresse, et en tenant compte des droits des autres personnes éventuellement visibles sur les mêmes séquences et des circonstances du dossier, vous devez lui permettre de visionner les séquences transférées ou lui en fournir une copie.

L'accès aux informations minimales visées à l'article 13 du règlement doit être accordé gratuitement. La gratuité de l'accès devrait également être la politique par défaut pour les informations plus détaillées ou l'accès aux enregistrements de vidéosurveillance. Cette politique par défaut peut toutefois être modifiée moyennant motivation dans les cas où le nombre de demandes d'accès augmente de façon significative, et ce afin de décourager les demandes purement vexatoires ou fantaisistes. Dans ce cas, il est possible de demander le versement d'un *montant raisonnable* pour la remise de copies d'enregistrements ou pour permettre aux

personnes concernées de visionner les enregistrements, de façon à couvrir les coûts afférents à cet accès. Ces frais ne doivent pas être excessifs et ne doivent pas servir à décourager les demandes d'accès légitimes. La somme à payer pour obtenir l'accès doit être indiquée dans la politique de vidéosurveillance.

Il convient de réagir sans retard aux demandes d'accès. L'accès doit être accordé dans la mesure du possible, ou une autre réponse concrète (et pas seulement un accusé de réception) doit être donnée à la requête dans un délai de 15 jours calendrier.

Exemple:

Un membre du personnel introduit une demande d'accès à un enregistrement en précisant la date et l'endroit de l'enregistrement. Il n'invoque pas l'urgence et ne précise pas la raison de sa demande ni s'il souhaite obtenir une copie de l'enregistrement ou simplement le visionner. Il fournit par ailleurs toutes les informations nécessaires (preuve d'identité, photo). Quelques jours après la demande, vous trouvez l'enregistrement. Sur cet enregistrement, plusieurs autres personnes sont visibles à l'arrière-plan. En quelques jours supplémentaires, vous masquez les images des personnes à l'arrière-plan et vous envoyez un courriel à l'employé pour l'inviter à prendre rendez-vous afin de venir visionner la séquence dans vos locaux. Si l'employé qui a introduit la demande d'accès répond sans traîner à votre courriel, l'accès aura été accordé dans les 15 jours.

Dans les situations plus complexes, il est possible d'envoyer un accusé de réception accompagné d'autres informations concernant la raison du retard et la date prévue pour la phase suivante de la procédure. Cependant, et quelle que soit la complexité du dossier, l'autorisation d'accès (ou la réponse définitive et concrète refusant l'accès) ne doit pas être retardée au-delà du délai maximal de trois mois prévu par le règlement[43]. Dans la plupart des cas, l'accès devrait être accordé beaucoup plus rapidement.

Si la demande est urgente, elle doit recevoir une réponse le plus rapidement possible. Dans la mesure du possible, il convient de respecter les échéances demandées expressément ou qui découlent logiquement des circonstances du dossier.

En cas de doute quant à la réponse à donner à une demande spécifique, veuillez consulter le DPD. En cas de désaccord entre l'institution et la personne qui a introduit la demande d'accès, il convient de mettre en place une procédure simple et efficace de réclamation ou d'examen interne. Cette procédure doit être communiquée non seulement aux membres du personnel, mais aussi aux parties tierces qui en font la demande.

[43] Voir l'article 13 du règlement.

Le public doit être informé de la procédure d'examen aussi bien par la politique de vidéosurveillance que par la réponse donnée à la demande d'accès.

13 Responsabilité: garantir, vérifier et démontrer la bonne administration

Les institutions doivent adopter des politiques et des procédures visant à garantir que leur utilisation de la vidéosurveillance est conforme au règlement[44]. Afin d'assurer la transparence et la bonne administration, et d'apporter la preuve de la conformité de ses pratiques à ses employés, au CEPD et aux autres parties intéressées[45], chaque institution doit vérifier et documenter la conformité de ses pratiques aux dispositions des présentes lignes directrices.

Le CEPD recommande notamment à chaque institution

- d'adopter une politique de vidéosurveillance;
- de réaliser des audits périodiques et d'en documenter les résultats dans des rapports d'audit.

Par ailleurs, dans les cas visés au chapitre 3.2, il convient d'effectuer une analyse d'impact et d'en documenter les résultats dans un rapport d'analyse d'impact.

13.1 Politique de vidéosurveillance

La politique de vidéosurveillance doit

- présenter une vue d'ensemble du système de vidéosurveillance et décrire ses finalités;
- décrire l'utilisation du système, l'usage qui est fait des données à caractère personnel et les mesures de protection des données mises en place;
- confirmer expressément le respect du règlement et des lignes directrices;
- décrire toute déviation par rapport aux pratiques standard recommandées par les lignes directrices et en expliquer les raisons; et
- décrire les mesures de mises en œuvre éventuellement nécessaires.

La politique de vidéosurveillance est un document qui poursuit plusieurs objectifs. Elle doit répondre aux besoins suivants en matière de bonnes pratiques administratives:

- L'adoption de ce document sera souvent nécessaire pour compléter et spécifier la base juridique, et donc pour établir la légitimité de la

[44] Article 22, paragraphe 1 du règlement.

[45] Avis n° 168 du groupe de travail du 1er décembre 2009 sur «L'avenir de la protection de la vie privée», cité à la note 13 ci-dessus. Voir en particulier le chapitre 6, «Renforcement de la responsabilité des responsables du traitement des données».

vidéosurveillance[46].

- Le fait de mettre les bonnes pratiques par écrit et de réfléchir aux mesures supplémentaires à prendre permettra probablement d'améliorer les procédures et de garantir une meilleure conformité.
- L'adoption d'une politique et sa publication contribueront aussi au respect de l'obligation, imposée par le règlement, de communiquer au public les informations nécessaires pour garantir un traitement équitable.
- La politique définit un ensemble de règles permettant de mesurer la conformité (par exemple lors d'un audit).
- Enfin, en renforçant leur transparence et en apportant la preuve de leurs efforts de conformité, les institutions:
    - inspirent la confiance de leurs employés et des parties tierces;
    - contribuent à faciliter les consultations avec les parties prenantes; et
    - facilitent les interactions avec le CEPD.

Les institutions doivent publier leurs politiques de vidéosurveillance sur leur intranet et leurs sites internet. Si le document de base contient des informations confidentielles, une version non confidentielle doit être rendue publique.

Exemples:

Si nécessaire, les mesures de sécurité qui protègent votre système de vidéosurveillance, le plan détaillé du système indiquant l'emplacement exact des caméras et leurs spécifications de même que certaines mesures de surveillance spécifiques liées à la lutte contre le terrorisme peuvent être rédigées de façon sommaire pour éviter de mettre en péril la sécurité ou l'efficacité du système et de révéler des informations sensibles ou confidentielles.

L'annexe 1 fournit un modèle de politique de vidéosurveillance que les institutions peuvent modifier selon leurs besoins.

13.2 Audit de protection des données

Chaque institution doit vérifier et documenter la conformité de ses pratiques aux dispositions du règlement, à ces lignes directrices et à sa propre politique de vidéosurveillance par un audit de protection des données («**audit**»). Les résultats de cet audit doivent être synthétisés dans un rapport («**rapport d'audit**»)

L'audit poursuit un double objectif:

- vérifier l'existence d'une politique de vidéosurveillance documentée et à jour, et vérifier que cette politique est conforme au règlement et aux lignes directrices («**audit d'adéquation**»); et
- vérifier que les actions de l'organisation sont effectivement conformes à cette

[46] Article 5, point a) du règlement. Voir également l'article 8, paragraphe 2 de la Charte des droits fondamentaux de l'Union européenne et la jurisprudence en la matière.

politique de vidéosurveillance («**audit de conformité**»). Cette partie de l'audit implique de vérifier que le personnel a conscience de l'existence de la politique, qu'il la comprend, qu'il respecte ses dispositions et que cette politique fonctionne réellement et de façon efficace.

La première préoccupation de l'audit d'adéquation est de confirmer l'existence d'une politique documentée de gestion des questions de protection des données, et de vérifier que cette politique répond correctement à toutes les exigences du règlement et des lignes directrices. L'audit de conformité porte sur l'application pratique de cette politique et sur son efficacité.

Entre autres avantages, l'audit:

- facilite le respect des règles de protection des données;
- sensibilise la direction et le personnel aux questions de protection des données;
- fournit des informations en vue d'un éventuel réexamen de la politique de vidéosurveillance; et
- réduit le risque d'erreurs susceptibles d'entraîner une plainte.

Le rapport d'audit doit:

- indiquer la date et la portée de l'audit, les membres de l'équipe d'audit, etc.
- résumer les principales observations de l'audit et indiquer les non-conformités éventuellement identifiées;
- suggérer des mesures de correction éventuelles; et
- préciser la nature et le calendrier prévu pour le suivi convenu.

Une partie de l'audit d'adéquation peut être réalisée à distance sur la base de documents écrits. Pour un audit complet par contre, il est essentiel de faire des visites sur sites, d'examiner les logiciels et le matériel de vidéosurveillance, les avis de protection des données affichés sur place, le registre de conservation des données et le registre des transferts, les fichiers d'archive, les demandes d'accès et les autres documents disponibles concernant l'utilisation du système, et d'avoir des discussions avec la direction et avec les membres du personnel.

L'audit peut être réalisé en interne (auto-audit) ou confié à une partie tierce indépendante (audit par un tiers). L'auditeur tiers peut être, par exemple, une autre institution si l'audit est réalisé sur une base réciproque. Dans ce cas, les institutions contrôlent mutuellement leurs pratiques, ce qui peut encourager le *benchmarking* et l'adoption des meilleures pratiques.

Autant que possible, il convient d'éviter que les auditeurs aient un lien avec la partie de l'organisation faisant l'objet de l'audit (généralement l'unité de sécurité). Le CEPD recommande aussi vivement de confier un rôle important au DPD de l'institution dans la conception et la mise en œuvre des procédures d'audit de l'institution et de lui donner des moyens suffisants pour s'acquitter de cette tâche. Pour les auto-audits, le CEPD recommande d'inclure autant que possible les auditeurs internes de l'institution dans l'équipe d'audit et de leur donner une formation adéquate à la protection des données et aux présentes lignes directrices. La procédure d'audit ne

doit en aucun cas nuire à l'indépendance du DPD. Les DPD et leur personnel doivent jouer un rôle actif dans l'audit et dans son suivi, qu'ils fassent ou non formellement partie de l'équipe d'audit.

Le CEPD peut émettre des recommandations supplémentaires sur la réalisation des audits. Ces recommandations peuvent comporter des listes de contrôle de conformité ainsi que des conseils supplémentaires en matière de méthodologie d'audit.

Un audit doit être réalisé avant le lancement du système de vidéosurveillance, mais aussi à intervalles réguliers par la suite, tous les 2 ans au moins et aussi à chaque fois qu'un changement de circonstances important justifie une réévaluation. Les mises à niveau importantes du système nécessitent normalement une réévaluation.

14 Externalisation et parties tierces

14.1 Externalisation de la vidéosurveillance

Si une institution externalise une partie de ses activités de vidéosurveillance, elle reste toutefois responsable en tant que «responsable du traitement». Il convient donc de faire preuve d'une diligence raisonnable dans le choix des sous-traitants et d'adopter une approche proactive du contrôle de la conformité aux règles.

Les obligations du sous-traitant en matière de protection des données doivent être précisées par écrit et d'une façon légalement contraignante. Cela signifie en général qu'un contrat écrit doit être conclu entre l'institution et la société extérieure. La société extérieure doit également avoir des contrats écrits avec ses propres sous-traitants.

Le contrat et le cahier de charges de l'appel d'offres doivent préciser l'obligation, pour le sous-traitant, de respecter:

- le règlement;
- les présentes lignes directrices;
- la politique de vidéosurveillance de l'institution; et
- tout autre conseil donné par le CEPD, par exemple dans le cadre d'un contrôle préalable éventuel ou d'une procédure de plainte ou à la suite d'une inspection ou d'une consultation.

Le contrat et le cahier de charges de l'appel d'offres doivent également mentionner clairement et spécifiquement les obligations de la société extérieure concernant:

- la sécurité;
- la confidentialité; et
- son obligation d'agir uniquement sur la base des instructions de votre institution[47].

[47] Voir les articles 22 et 23 du règlement.

La société extérieure doit également offrir une formation adéquate à son personnel, y compris en matière de protection des données. Tout sous-traitant direct ou indirect doit être lié par les mêmes obligations que le contractant direct. L'institution doit avoir le droit de refuser le choix d'un sous-traitant en cas de doute raisonnable quant à la capacité de celui-ci de répondre aux exigences en matière de protection des données.

Si nécessaire, il convient de donner des instructions détaillées au sous-traitant pour garantir le respect des mesures de protection prévues par le règlement et par les présentes lignes directrices. À cet égard, il convient de veiller en particulier à ce que le public et le personnel de l'institution soient correctement informés des règles de protection des données.

14.2 Vidéosurveillance par des parties tierces

Il arrive que la vidéosurveillance ne soit pas assurée par l'institution ni par un sous-traitant en son nom, mais par le propriétaire auquel l'institution loue ses locaux ou par un sous-traitant travaillant pour le compte du propriétaire. Il existe parfois des montages contractuels complexes impliquant plusieurs contrats de location et de sous-location et/ou plusieurs sociétés et sous-traitants, et il se peut que l'institution n'ait qu'une influence contractuelle très limitée ou nulle sur l'exploitant du système de vidéosurveillance.

Exemple:

L'institution A loue un étage d'un grand bâtiment à l'institution B, qui occupe les autres étages du bâtiment. L'institution B, quant à elle, loue les locaux au propriétaire du bâtiment, la société C. La société C a confié la maintenance du bâtiment à la société D. La société D. quant à elle, sous-traite la sécurité du bâtiment, y compris l'exploitation du système de vidéosurveillance, à la société spécialisée E. Il existe alors quatre niveaux de relations contractuelles entre l'institution et l'entité effectivement chargée de la vidéosurveillance.

Néanmoins, et même si l'institution ne sera pas considérée comme le «responsable du traitement» dans la plupart des situations de ce genre, elle doit jouer un rôle proactif et faire des efforts raisonnables pour s'assurer que le responsable du traitement pratique la vidéosurveillance dans le respect des présentes lignes directrices. Elle devrait, par exemple, négocier avec le propriétaire (ou avec les autres acteurs concernés si nécessaire) pour garantir le respect des mesures de protection essentielles prévues par le règlement (par exemple l'affichage d'avis sur place et la publication d'informations plus détaillées sur l'intranet et le site internet de l'institution).

15 Dispositions transitoires et mises à jour futures

Les lignes directrices s'appliquent aussi bien aux systèmes de vidéosurveillance déjà en place qu'aux systèmes encore à installer et aux activités futures. Chaque

institution est tenue de mettre ses pratiques existantes en conformité avec les lignes directrices pour le 1er janvier 2011. La mise en conformité des systèmes existants impose aux institutions, pour cette date:

- de faire l'inventaire de leurs pratiques existantes;
- d'identifier les mesures supplémentaires nécessaires pour garantir la conformité; et
- de mettre en œuvre toutes les mesures nécessaires pour garantir la conformité.

Dans la plupart des cas, cette analyse ex-post ne doit pas être un exercice lourd et compliqué. Elle ne doit en aucun cas imposer un fardeau administratif excessif. À vrai dire, de nombreuses institutions qui ont discuté de leurs systèmes de vidéosurveillance avec leurs DPD par le passé constateront probablement que leurs pratiques existantes suivent déjà dans une large mesure les recommandations des lignes directrices. Il leur restera donc simplement à vérifier et à confirmer ces pratiques par écrit. En outre, et c'est un point important, la vérification permettra également aux institutions d'identifier des ajustements ciblés et spécifiques qui leur permettront de renforcer encore leur conformité.

Pour effectuer cette analyse ex-post de la façon la plus efficace possible, le CEPD recommande d'adopter une approche globale. Chaque institution procède alors à un seul exercice par lequel:

- elle vérifie (via un audit formel ou un exercice informel d'établissement des faits) l'adéquation et la conformité des pratiques existantes par rapport au règlement et aux lignes directrices;
- elle rédige (ou met à jour) sa politique de vidéosurveillance; et enfin
- elle contrôle les pratiques revues par rapport à sa nouvelle politique, aux lignes directrices et au règlement via un audit formel d'adéquation et de conformité.

Si cela s'avère nécessaire ou utile, une analyse d'impact ex-post devrait également être préparée dans le cadre de la même analyse.

15.1. Analyse ex-post du statut de conformité et contrôle préalable ex-post[48]

Le DPD doit informer le CEPD du statut de conformité de son institution pour la même date. Il suffit pour cela d'envoyer un simple courrier au CEPD. Ce courrier doit

- confirmer que l'institution a adopté une politique de vidéosurveillance et effectué un audit;
- préciser si l'institution a également effectué une analyse d'impact; et
- si l'institution estime qu'un contrôle préalable ex-post est nécessaire, et pour quelle raison.

[48] On entend par «contrôle préalable ex-post» la vérification de systèmes existants, alors que le «véritable» contrôle préalable au sens de l'article 27 du règlement désigne l'analyse de nouveaux systèmes (ou de modifications de systèmes existants) avant leur mise en place.

Les documents suivants doivent être joints à la lettre:

- la politique de vidéosurveillance (avec ses annexes);
- le rapport d'audit; et
- le cas échéant, le rapport de l'analyse d'impact.

Si, malgré les efforts déployés par une institution, celle-ci ne parvient pas à assurer la conformité de certains aspects spécifiques pour le 1er janvier 2011, elle doit adopter un plan l'engageant à arriver pas à pas à une conformité complète. Ce plan doit expliquer les raisons du retard de conformité et identifier les dates prévues et les mesures que l'institution compte prendre pour se mettre en conformité le plus rapidement possible. Ce plan doit être soumis au CEPD pour le 1er janvier 2011, en même temps que les autres documents énumérés ci-dessus.

Étant donné que ces documents doivent déjà contenir tous les éléments à inclure normalement dans le formulaire de notification de contrôle préalable au CEPD et afin d'éviter les efforts redondants, il n'est pas nécessaire de soumettre une autre notification de contrôle préalable au CEPD. L'institution doit par contre indiquer clairement si elle demande un contrôle préalable ex-post, et pour quelle raison. Le CEPD encourage les institutions à se mettre en conformité et à lui communiquer leur statut de conformité avant l'échéance.

En cas de doute, le CEPD peut être consulté à propos de toute difficulté survenant au cours de la période transitoire.

À partir du 1er janvier 2011, et après avoir reçu les documents demandés, le CEPD établira un calendrier de traitement des notifications de contrôle préalable ex-post. En fonction du nombre et de la qualité des notifications de contrôle préalable ex-post reçues, de l'éventail de problèmes rencontrés et d'autres facteurs pertinents, le CEPD pourra émettre des avis individuels ou des avis communs portant sur plusieurs institutions et/ou problèmes. Cette procédure pourra aussi comporter des contrôles ou des inspections sur site.

À un stade ultérieur ou parallèlement au traitement des notifications de contrôle préalable, le CEPD peut lancer des enquêtes et/ou des inspections portant sur les pratiques de certaines institutions, même si ces pratiques ne nécessitent pas de contrôle préalable. En fonction du degré de conformité des institutions, de l'éventail de problèmes rencontrés et d'autres facteurs pertinents, le CEPD pourra émettre des recommandations supplémentaires soit à titre individuel, soit à plusieurs institutions en même temps si ces recommandations portent sur des problèmes communs.

15.2. Notifications de contrôle préalable ex-post en suspens

En raison des changements requis par les institutions pour mettre leurs pratiques en conformité avec la présente protection des données, le CEPD clôturera toutes les procédures de contrôle préalable ex-post dont les notifications ont été soumises avant la publication des présentes lignes directrices et qui ont été suspendues en attendant l'adoption des lignes directrices. Les institutions dont les notifications de

contrôle préalable ont ainsi été clôturées doivent communiquer leur statut de conformité au CEPD dans le respect des règles générales et des échéances généralement applicables.

Sur demande expresse, et afin d'aider les institutions dans leurs efforts de conformité, le CEPD peut émettre des recommandations préliminaires sur la base de la notification de contrôle préalable et d'autres documents soumis par l'institution dans le passé. Ces recommandations seront basées uniquement sur la documentation reçue, sans analyse approfondie.

15.3. Notifications de contrôle préalable pour les nouveaux systèmes

En ce qui concerne les notifications de «véritable» contrôle préalable pour les nouveaux systèmes, ces notifications doivent être soumises le plus tôt possible durant la phase de planification, indépendamment de la période transitoire ou du calendrier établi pour les analyses ex-post. Le CEPD traitera ces notifications en urgence.

15.4. Révision des lignes directrices

Le CEPD peut publier des versions révisées des présentes lignes directrices lorsque des changements importants de circonstances l'exigent. Les circonstances susceptibles de provoquer une révision sont notamment:

- l'évolution des pratiques de vidéosurveillance au sein des institutions et sur le plan international, y compris les évolutions technologiques;
- l'évolution des règles internationales en matière de vidéosurveillance;
- les apprentissages tirés de l'application de ces lignes directrices et des commentaires reçus.

Annexe 1: Modèle de politique de vidéosurveillance

Politique de vidéosurveillance de [Agence]

Adoptée sur décision du directeur le **[31 mai 2010]**

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

Notre Agence 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 l'Agence et les mesures de garanties prises par l'Agence afin de 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. Comment faisons-nous en sorte que notre système soit conçu en tenant compte des préoccupations de respect de la vie privée et de protection des données et qu'il respecte la législation en matière de protection des données?

2.1. Révision du système existant. Notre Agence utilisait déjà un système de vidéosurveillance avant la publication des lignes directrices en matière de vidéosurveillance par le Contrôleur européen de la protection des données (les «**lignes directrices**»), le _____ 2010. Depuis cette date, nous avons revu nos procédures conformément aux recommandations contenues dans les lignes directrices (Lignes directrices, chapitre 15). **[hyperlien vers les lignes directrices sur le site internet du CEPD]**

2.2. Statut de conformité. L'Agence traite les images conformément aux lignes directrices et au règlement (CE) nº 45/2001 relatif à la protection des données à caractère personnel par les institutions et organes communautaires. **[Si vous vous écartez de n'importe quelle recommandation des lignes directrices, votre politique de vidéosurveillance doit l'indiquer clairement et justifier cette déviation.]**

2.3. Auto-audit. Le système a fait l'objet d'un audit interne par l'Agence. Le **rapport d'audit** est joint à l'**annexe 1**.

2.4. Notification du statut de conformité au CEPD. Étant donné la portée limitée du système, il n'a pas été nécessaire de procéder à une analyse d'impact formelle (Lignes directrices, chapitre 3.2) ni de soumettre une notification de contrôle préalable au CEPD (Lignes directrices, chapitre 4.3). **[Remarque: si votre institution a effectué une analyse d'impact, le rapport de cette analyse doit**

également être annexé à votre politique de vidéosurveillance et les principales difficultés et observations doivent être présentées dans la politique elle-même. De même, si le CEPD a émis un avis de contrôle préalable, celui-ci doit aussi être annexé et la politique elle-même doit contenir une synthèse des principales recommandations du CEPD et des suites que vous avez données à ces recommandations.]

Parallèlement à l'adoption de cette vidéosurveillance, nous avons également communiqué notre statut de conformité au CEPD en lui envoyant une copie de notre politique de vidéosurveillance et de notre premier rapport d'audit.

2.5. Contacts avec l'autorité de protection des données compétente dans l'État membre. L'autorité de protection des données compétente en [**insérer pays**] a été informée, et ses préoccupations et recommandations ont été prises en considération. En particulier, à la fois l'avis affiché sur place et cette politique de vidéosurveillance sont également disponibles en **[langue[s] locales]**.

2.6. Décision du directeur 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 directeur de l'Agence après avoir consulté:

- le chef de l'unité de sécurité de l'Agence;
- le délégué à la protection des données de l'Agence; et
- le comité du personnel.

Durant ce processus de prise de décision, l'Agence

- a démontré et documenté la nécessité de recourir à un système de vidéosurveillance tel que proposé par cette politique;
- a envisagé les alternatives et conclu que le maintien du système de vidéosurveillance actuel, après l'adoption en matière de protection des données proposées dans cette politique, était nécessaire et proportionnée au regard des objectifs décrits au chapitre 1 (voir Lignes directrices, chapitre 5); et
- a réagi aux préoccupations exprimées par le DPD et par le comité du personnel (voir Lignes directrices, chapitre 4).

2.7 Transparence. Cette politique de vidéosurveillance existe en deux versions, une version confidentielle à usage restreint et la présente version publiée sur notre site internet et sur l'intranet de l'Agence aux adresses [**adresses intranet et internet**]. La présente version publique de la politique de vidéosurveillance contient parfois des informations sommaires concernant certains thèmes ou annexes. La présence d'informations sommaires est toujours indiquée 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).

2.8. Contrôles périodiques. L'unité de 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 2012. Lors de ces contrôles périodiques, nous vérifierons:

- que l'utilisation du système de vidéosurveillance reste nécessaire;
- que le système répond encore à son objectif initial; et
- qu'il n'existe toujours pas d'alternatives adéquates.

Les contrôles périodiques couvriront également toutes les questions abordées par le premier rapport. Ils vérifieront notamment si notre 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 contrôles périodiques seront également jointes à l'**annexe 1** de cette politique de vidéosurveillance.

2.9. Solutions technologiques respectueuses de la vie privée. Nous avons également déployé les solutions technologiques respectueuses de la vie privée suivantes (voir Lignes directrices, chapitre 3.4):

[Énumérer et décrire les solutions mises en œuvre]

3. Quels sont les endroits sous surveillance?

Le système de vidéosurveillance se compose de **[sept caméras fixes]**. **Un plan indiquant l'emplacement des caméras** est joint à l'**annexe 2**.

Sur ces **[sept caméras, six]** sont situées aux entrées et sorties de notre bâtiment, y compris l'entrée principale, les sorties de secours et les sorties en cas d'incendie, et l'accès au parking. Une caméra est également installée au pied des escaliers du parking.

Il n'y a pas d'autre caméra ailleurs, que ce soit à l'intérieur du bâtiment ou en dehors de celui-ci. Nous ne surveillons pas non plus les endroits où les personnes peuvent s'attendre à un respect plus important de leur vie privée, par exemple les bureaux individuels, les espaces de détente, les locaux sanitaires, etc. (voir Lignes directrices, chapitre 6.8). L'emplacement des caméras a été choisi avec soin de façon à limiter le plus possible la surveillance de zones ne présentant aucun intérêt pour l'objectif recherché (Lignes directrices, chapitre 6.1).

La surveillance à l'extérieur de notre bâtiment et sur le territoire de [**insérer le nom de l'État membre où se situe votre institution**] est limitée au strict minimum, comme le recommande le chapitre 6.5 des Lignes directrices.

4. Quelles informations personnelles collectons-nous, et dans quel but?

4.1. Description sommaire et spécifications techniques détaillées du système. Le système de vidéosurveillance est un système statique traditionnel. Il enregistre

des images numériques et est doté de détecteurs de mouvement. Il enregistre tous les mouvements détectés par les caméras dans chaque zone surveillée ainsi que l'heure, la date et l'endroit. Toutes les caméras fonctionnent 24 heures sur 24, 7 jours sur 7. Dans la plupart des cas, la qualité des images permet d'identifier les personnes se trouvant dans le champ des caméras (voir Lignes directrices, chapitre 6.4). Les caméras sont toutes fixes (pas de caméras à balayage horizontal, vertical et zoom). Les opérateurs ne peuvent donc pas les utiliser pour zoomer sur une cible ni pour suivre des personnes.

Nous n'utilisons pas d'équipements de vidéosurveillance de haute technologie ni de vidéosurveillance intelligente (voir le chapitre 6.9 des Lignes directrices) et notre système n'est pas interconnecté avec d'autres systèmes (chapitre 6.10). Nous n'avons pas recours à une surveillance dissimulée (chapitre 6.11), à des enregistrements sonores ni à des «caméras de surveillance parlantes» (chapitre 6.12). **Les spécifications techniques** des caméras et **de l'ensemble du système de vidéosurveillance** (matériel et logiciel compris) sont jointes à l'**annexe 3**.

4.2. Objectif de la surveillance. L'Agence utilise son système de vidéosurveillance à des fins de sécurité et de contrôle des accès uniquement. Le système de vidéosurveillance facilite le contrôle des accès à nos bâtiments et contribue à garantir la sécurité de nos bâtiments, la sécurité de notre personnel et des visiteurs ainsi que l'intégrité des biens et des informations présents dans les locaux. Il s'ajoute aux autres systèmes de sécurité physique tels que les systèmes de contrôle des accès et les systèmes de contrôle des intrusions physiques. Il fait partie des mesures prises dans le cadre de nos politiques de sécurité plus générales 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 l'Agence, à ses visiteurs ou à son personnel et à contrer les menaces pour la sécurité des visiteurs et du personnel travaillant dans les locaux (par ex. incendie, agression physique).

4.3. 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 employés. 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, dans le cadre d'une enquête criminelle ou disciplinaire formelle, comme l'indique le chapitre 6.5 ci-dessous (voir les chapitres 5.7, 5.8 et 10.3 des Lignes directrices).

4.4. Pas de surveillance *ad hoc* prévue. Nous ne prévoyons aucune opération de surveillance *ad hoc* qui nécessiterait une planification à ce stade (voir Lignes directrices, chapitre 3.5).

4.5. Webcams. Nous n'utilisons pas de webcams (voir le chapitre 5.10 des Lignes directrices).

4.6. Pas de collecte de catégories spéciales de données. Nous ne collectons pas de catégories spéciales de données (chapitre 6.7 des Lignes directrices).

5. Quelle est la légitimation et la base juridique de la vidéosurveillance?

L'utilisation de notre système de vidéosurveillance est nécessaire pour la gestion et le fonctionnement de notre Agence (aux fins de sécurité et de contrôle des accès décrites au chapitre 4.2 ci-dessus). Notre recours à la vidéosurveillance est donc légitime (voir le chapitre 5.2 des Lignes directrices. La présente politique de vidéosurveillance fournit une base juridique plus détaillée et spécifique pour la vidéosurveillance. Cette politique s'inscrit quant à elle dans un ensemble plus large de politiques de sécurité adoptées par notre Agence.

6. Qui a accès aux informations, et à qui sont-elles divulguées?

6.1. Personnel de sécurité interne et gardiens de sécurité extérieurs. Les séquences enregistrées sont accessibles uniquement à notre personnel de sécurité interne. Les images en direct sont également accessibles aux gardiens de sécurité en service. Ces gardiens de sécurité sont employés par une société de sécurité extérieure. Le **contrat conclu avec cette entreprise de sécurité** est joint à l'**annexe 4**.

6.2. Droits d'accès. La politique de sécurité de l'Agence en matière de vidéosurveillance (voir le chapitre 7 ci-dessous et l'annexe 7) précise et documente clairement qui a accès aux séquences de vidéosurveillance et/ou à l'architecture technique du système de vidéosurveillance, la raison de cet accès et la nature précise des droits d'accès. Ce document précise notamment qui a le droit de:

- visionner les séquences en temps réel;
- visionner les séquences enregistrées; ou
- copier,
- télécharger,
- supprimer ou
- modifier une séquence.

6.3. Formation à la protection des données. Tous les membres du personnel possédant un droit d'accès, y compris les gardiens de sécurité extérieurs, ont reçu leur première formation à la protection des données le **[15 mai 2010]**. 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 le chapitre 8.2 des Lignes directrices).

6.4. Accords de confidentialité. Au terme de la formation, tous les membres du personnel concernés ont également signé un accord de confidentialité. Cet accord a également été signé par la société extérieure. Des copies des **accords de confidentialité** sont jointes à l'**annexe 5** (voir le chapitre 8.3 des Lignes directrices).

6.5. Transferts et divulgations. Tous les transferts et toutes les divulgations en dehors de l'unité de sécurité sont documentés et font l'objet d'une évaluation rigoureuse de la nécessité de ces transferts et de la compatibilité de l'objectif de ces transferts avec la finalité originale de sécurité et de contrôle d'accès du traitement (voir le chapitre 10 des Lignes directrices). **Le registre des séquences conservées et des transferts** est joint à **l'annexe 6** (voir les chapitres 10.5 et 7.2 des Lignes directrices). Le DPD de l'Agence est systématiquement consulté. **[Si vous pratiquez des transferts routiniers n'impliquant pas le DPD, veuillez en décrire les principes en détail dans cette politique de vidéosurveillance.]**

Aucun accès n'est donné à la direction ni au service des ressources humaines. **[Dans le cas contraire, veuillez fournir des exemples de transferts de ce type. Décrivez également les règles qui régissent quelles données peuvent être transférées à quelles personnes et dans quelles circonstances.]**

Un accès peut être accordé à la police locale si cela s'avère nécessaire pour enquêter sur des délits ou pour mener des poursuites. Dans le passé, la police a pu accéder à quelques reprises à des séquences de vidéosurveillance afin d'enquêter sur des vols de vélos depuis les porte-vélos situés à l'entrée du garage. Au cours des [**cinq]** dernières années pour lesquelles nous avons conservé la liste des transferts, aucun autre accès n'a été accordé à la police. **[Dans le cas contraire, veuillez fournir des exemples de transferts de ce type. Décrivez également les règles qui régissent quelles données peuvent être transférées, à qui et dans quelles circonstances.]**

Dans des circonstances exceptionnelles, un accès peut également être accordé aux organes suivants:

- l'Office européen de lutte antifraude (**OLAF**), dans le cadre d'une enquête menée par l'OLAF;
- 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
- les organes chargés de mener une enquête interne ou une procédure disciplinaire au sein de l'institution.

Ces transferts sont acceptables s'il y 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 nous avons conservé la liste des transferts, aucun transfert n'a été autorisé pour l'une des raisons énumérées ci-dessus.

7. Comment protégeons-nous et sauvegardons-nous les informations?

Un certain nombre de mesures techniques et organisationnelles ont été prises afin de protéger la sécurité du système de vidéosurveillance, y compris les données personnelles. Ces mesures sont décrites en détail dans une politique de sécurité

spécifique consacrée à ce processus («**Politique de sécurité en matière de vidéosurveillance**»), jointe à l'**annexe 7**.

La politique de sécurité de l'Agence en matière de vidéosurveillance a été créée conformément au chapitre 9 des lignes directrices du CEPD en matière de vidéosurveillance.

Nous avons notamment pris les mesures suivantes:

- Les serveurs contenant les images enregistrées sont hébergés dans des locaux sécurisés protégés par des mesures de sécurité physiques; des pare-feu de réseau protègent le périmètre logique de l'infrastructure informatique; et les principaux systèmes informatiques contenant les données bénéficient d'une sécurité renforcée.
- Les mesures administratives imposent à tous les membres du personnel ayant accès au système (y compris les personnes chargées de la maintenance du matériel et des systèmes) de posséder une accréditation de sécurité.
- Tous les membres du personnel (externes et internes) ont signé des accords de confidentialité et de non-divulgation.
- Les utilisateurs ont accès uniquement aux informations strictement nécessaires pour l'exécution de leur travail.
- Seul l'administrateur du système désigné expressément par le responsable du traitement est habilité à accorder, modifier ou supprimer les droits d'accès de toute autre personne. L'octroi, la modification et la suppression de droits d'accès se font dans le respect des critères définis par la politique de sécurité en matière de vidéosurveillance (voir annexe 7).
- La politique de sécurité en matière de vidéosurveillance contient une liste à jour de toutes les personnes ayant accès au système à tout moment et décrit en détail la portée de leurs droits d'accès.

8. Pendant combien de temps conservons-nous les données?

Les images sont conservées pendant 48 heures au maximum. Toutes les images sont ensuite effacées. Certaines images peuvent être conservées 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. Une copie du **registre de conservation et des transferts** est jointe à **l'annexe 6** (voir le chapitre 7 des Lignes directrices).

Le système est également contrôlé en direct 24 heures sur 24 par le gardien de sécurité en service dans le local de réception du rez-de-chaussée.

9. Comment informons-nous le public?

9.1. Approche à plusieurs niveaux. Les informations relatives à la vidéosurveillance sont communiquées au public de façon complète et effective (voir

le chapitre 11 des Lignes directrices). Nous avons adopté à cette fin une approche à plusieurs niveaux associant les deux méthodes suivantes:

- des avis affichés sur place permettant d'informer le public de la vidéosurveillance et de lui fournir les informations essentielles relatives au traitement; et
- la publication de cette politique de vidéosurveillance sur notre intranet et sur notre site internet à l'intention de tous ceux qui souhaitent en savoir plus sur les pratiques de vidéosurveillance de notre institution.

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

Nous affichons également des avis à proximité des zones sous surveillance. Nous avons affiché un avis à proximité de l'entrée principale, à l'entrée des ascenseurs dans le parking et à l'entrée du parking.

L'avis de protection des données affiché sur place par l'Agence est joint à l'**annexe 8**.

9.2. Notification individuelle spécifique. Par ailleurs, les personnes identifiées sur caméra (par exemple par le personnel de sécurité dans le cadre d'une enquête de sécurité) doivent 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,
- conservé au-delà de la période de conservation normale,
- transféré en dehors de l'unité de sécurité; *ou*
- l'identité de la personne est communiquée à une personne extérieure à l'unité de sécurité.

La notification peut parfois être retardée temporairement, par exemple si ce délai est nécessaire pour l'enquête ou pour la prévention, la détection ou la poursuite de délits[49]. Dans ce cas, le DPD est systématiquement consulté afin de garantir le respect des droits de la personne concernée.

10. Comment les membres du public peuvent-ils vérifier, modifier ou supprimer les informations les concernant? Les membres du public ont le droit d'accéder aux

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

données personnelles les concernant que nous détenons, et de corriger et compléter ces données. Toute demande d'accès, de rectification, blocage et/ou suppression de données à caractère personnel doit être adressée à M^{me}/M. _____, chef de l'unité _____ **[adresse électronique et numéro de téléphone]**. Cette personne peut également être contactée pour toute autre question relative au traitement de données à caractère personnel.

Dans la mesure du possible, l'unité de 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 de trois mois au maximum. L'unité doit faire 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 ce genre doit faire la preuve de son identité (par exemple en présentant sa carte d'identité avant le visionnage) et, dans la mesure du possible, indiquer 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 visionnées.

À l'heure actuelle, nous ne demandons pas de contribution financière aux personnes qui demandent de visionner leurs images ou d'en recevoir une copie. Nous nous réservons 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 45/2001. Par exemple, au terme d'une évaluation au cas par cas, nous pouvons arriver à la conclusion qu'il est nécessaire de refuser l'accès pour protéger 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 45/2001 ont été violés du fait du traitement de ses données personnelles par l'Agence, Avant d'en arriver là, nous recommandons aux personnes concernées d'essayer d'obtenir satisfaction en contactant:

- le chef de l'unité de sécurité (voir les coordonnées de contact ci-dessus); et/ou
- le délégué à la protection des données de l'Agence **[insérer le nom, le**

numéro de téléphone et l'adresse électronique]

Les membres du personnel peuvent également demander une évaluation par l'autorité qui les a engagés au titre de l'article 90 du statut du personnel.

[Détails de la procédure de recours interne, y compris calendrier et coordonnées de contact.]

* * *

Annexes à la politique de vidéosurveillance:

- Le **rapport d'audit** est joint à l'**annexe 1**. L'annexe 1 contiendra également les **contrôles périodiques**.
- Un plan indiquant l'emplacement des caméras est joint à l'**annexe 2**.
- Les **spécifications techniques** des caméras et de l'ensemble du système de vidéosurveillance (matériel et logiciel compris) sont jointes à l'**annexe 3**.
- Le **contrat conclu avec l'entreprise de sécurité** externe est joint à l'**annexe 4**.
- Des copies des **accords de confidentialité** sont jointes à l'**annexe 5** (voir le chapitre 8.3 des Lignes directrices).
- **Le registre de conservation et des transferts** est joint à **l'annexe 6** (voir les chapitres 10.5 et 7.2 des Lignes directrices).
- Un certain nombre de mesures techniques et organisationnelles ont été prises afin de protéger la sécurité du système de vidéosurveillance, y compris les données personnelles qu'il contient. Ces mesures sont décrites en détail dans une politique de sécurité spécifique consacrée au traitement («**Politique de sécurité en matière de vidéosurveillance**»), jointe à l'**annexe 7**.
- **L'avis de protection des données affiché sur place** par l'Agence est joint à l'**annexe 8**.

Annexe 2: Exemple d'avis de protection des données affiché sur place

[Insérez votre pictogramme de vidéosurveillance: vous pouvez envisager, par exemple, le pictogramme ISO ou le pictogramme utilisé habituellement à l'endroit où se situe votre institution.]

Pour votre sécurité, ce bâtiment et son voisinage immédiat sont placés sous vidéosurveillance. Aucune image n'est enregistrée. **[Alternative: Les images sont conservées pendant 48 heures.]**

Pour de plus amples informations, veuillez consulter www.nomdedomainedevotreinstitution.cctv ou contacter l'unité de sécurité de l'Agence à **[numéro de téléphone et adresse électronique].**

[Si nécessaire, inclure des versions multilingues.]