

**Politique de vidéoprotection du Parlement européen**

**adoptée par la  
directrice générale de la sécurité et de la protection du  
Parlement européen**

**Mise à jour en janvier 2022**

## Table des matières

1. Champ d'application .....	3
2. Limitation des finalités .....	3
3. Bases juridiques .....	3
4. Zones sous protection .....	4
4.1. Vidéoprotection ad hoc .....	4
5. Informations à caractère personnel collectées et spécifications techniques du système .....	5
6. Accès aux images et divulgation des informations .....	5
6.1 Droits d'accès des agents et des administrateurs du système .....	5
6.2 Divulgation et transferts .....	6
7. Durée de conservation .....	6
8. Mesures de sécurité .....	6
9. Informations à fournir au public .....	7
10. Les droits des personnes concernées .....	7
11. Droit d'introduire une réclamation .....	9
12. Consultations et auto-audit en matière de protection des données .....	9

## 1. Champ d'application

La direction générale de la sécurité et de la protection du Parlement européen (ci-après «DG SAFE») utilise la vidéoprotection afin de **surveiller des zones, des événements, des activités ou des personnes grâce à un système de surveillance visuelle** appelé télévision en circuit fermé (CCTV).

La présente politique de vidéoprotection **décrit le système de vidéoprotection du Parlement européen, ses finalités et son utilisation, ainsi que les garanties** mises en place pour protéger les droits personnels des personnes concernées, comme le prévoit le règlement (UE) 2018/1725 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions de l'Union (ci-après le «règlement (UE) 2018/1725»).

## 2. Limitation des finalités

Le système de vidéoprotection contribue à garantir la sécurité et la sûreté conformément à la réglementation concernant la sécurité et la protection au Parlement européen<sup>1</sup>.

En effet, la DG SAFE s'appuie sur le système de vidéoprotection pour **prévenir, décourager ou gérer d'éventuelles menaces pour l'ordre et la sécurité, y compris l'accès physique non autorisé** aux bâtiments du Parlement européen ou à des zones d'accès restreint ou sensibles, à l'infrastructure informatique ou à des informations.

La DG SAFE peut en outre utiliser des séquences du système CCTV **dans le cadre d'enquêtes de sécurité et d'enquêtes auxiliaires** menées dans les limites de son mandat.

Tout transfert d'enregistrements de la CCTV intervient dans le strict respect des conditions énoncées à la section 6.2: «Divulgations et transferts»:

Le système de vidéoprotection n'est utilisé à d'autres finalités<sup>2</sup>.

## 3. Bases juridiques

L'utilisation du système de vidéoprotection du Parlement européen repose sur les bases juridiques suivantes:

- Parlement européen – décision du Bureau du 15 janvier 2018 sur la réglementation concernant la sécurité et la protection au Parlement européen, JO C 79 du 2 mars 2018, p. 3
- Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du

---

<sup>1</sup> Décision du Bureau du [Parlement européen](#) du 15 janvier 2018 sur la réglementation concernant la sécurité et la protection au Parlement européen, JO C 79 du 2 mars 2018, p. 3.

<sup>2</sup> Article 4 du règlement (EU) 2018/1725.

traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) 45/2001 et décision 1247/2002/CE

- Parlement européen – décision du Bureau du 17 juin 2019 sur les modalités d'exécution du règlement (UE) 2018/1725
- Parlement européen – décision du Bureau du 15 avril 2013 concernant les règles applicables au traitement des informations confidentielles par le Parlement européen, JO C 96 du 1.4.2014, p. 1
- Politique de sécurité de l'information au Parlement européen du 2 juin 2020, GEDA (D (2020) 14287)

#### **4. Zones sous protection**

La DG SAFE décide de l'emplacement des caméras et des angles de vue, et des zones soumises à la vidéoprotection, dans le plein respect des lignes directrices du Contrôleur européen de la protection des données<sup>3</sup>.

Les caméras sont positionnées à l'issue d'une évaluation des risques afin de veiller à ce qu'elles ne soient placées qu'aux endroits, zones et angles de vue les plus importants à l'intérieur et à l'extérieur des bâtiments et de garantir ainsi le respect de cette politique.

Plus spécifiquement, des caméras sont installées pour surveiller les points d'entrée et de sortie des bâtiments et à proximité immédiate de ceux-ci, y compris les zones d'accès public (telles que les entrées principales, les sorties de secours et les sorties en cas d'incendie, les entrées des parkings, les points de débarquement VIP, l'Esplanade, etc.). En outre, les caméras surveillent plusieurs escaliers ou points de connexion importants, ainsi que des zones stratégiques qui nécessitent une sécurité accrue, telles que des zones où se trouvent des biens de valeur, des informations confidentielles et sensibles, ou des «locaux sensibles» et des zones d'accès restreint.

Les zones pour lesquelles les attentes en matière de respect de la vie privée sont très élevées, telles que les bureaux individuels ou les espaces de loisirs, sont exclues de la surveillance.

La surveillance à l'extérieur des locaux du Parlement est limitée au périmètre minimal indispensable permettant de garantir la mise en œuvre de la présente politique et s'effectue dans le respect de la législation européenne et nationale applicable.

##### **4.1. Vidéoprotection ad hoc**

Dans des cas dûment justifiés, la DG SAFE peut utiliser une vidéoprotection ad hoc à des finalités spécifiques, et ce, pour une durée limitée.

---

<sup>3</sup> Ces lignes directrices sont disponibles via les liens suivants:

[https://edps.europa.eu/sites/edp/files/publication/10-03-17\\_video-surveillance\\_guidelines\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_fr.pdf) et [https://edps.europa.eu/data-protection/our-work/publications/guidelines/video-surveillance-follow\\_fr](https://edps.europa.eu/data-protection/our-work/publications/guidelines/video-surveillance-follow_fr)

Les caméras utilisées dans le cadre d'une vidéoprotection ad hoc sont installées sur demande écrite et moyennant autorisation écrite préalable de la directrice générale de la DG SAFE.

Le recours à une vidéoprotection ad hoc est limité à un mois. Toute prolongation requiert une nouvelle procédure dans les conditions susmentionnées.

Les caméras n'enregistrent qu'à des heures prédéfinies.

Les images enregistrées moyennant une vidéoprotection ad hoc ne seront pas stockées, sauf si elles sont jugées pertinentes aux fins d'une enquête de sécurité, auquel cas elles seront stockées dans le cadre de cette enquête.

Dans des cas dûment justifiés et après consultation du délégué à la protection des données, il est possible de prévoir une vidéoprotection ad hoc dissimulée.

## **5. Informations à caractère personnel collectées et spécifications techniques du système**

Le système de vidéoprotection du Parlement européen est un système CCTV standard. L'ensemble des caméras fonctionne 24 heures sur 24 et 7 jours sur 7.

La majorité des caméras n'enregistrent que des variations de pixels, ce qui signifie que l'accès à des images normales suppose que le système détecte un mouvement. Il enregistre tout mouvement détecté par les caméras dans la zone protégée, parallèlement à l'heure, à la date et au lieu. Dans ce cas, la qualité de l'image permet d'identifier des personnes ou d'autres détails sur les images.

Toutes les caméras, dotées ou non de détecteurs de mouvements, sont soumises aux mêmes mesures de sécurité strictes.

À l'heure actuelle, le système ne recourt pas à des enregistrements sonores au moyen du système CCTV. Le Parlement européen n'utilise pas de webcams à des fins de vidéoprotection.

Conformément à l'article 10 du règlement (UE) 2018/1725, le système de vidéoprotection n'est pas censé collecter des catégories particulières de données.

## **6. Accès aux images et divulgation des informations**

### **6.1 Droits d'accès des agents et des administrateurs du système**

Seule la directrice générale de la DG SAFE (ci-après «la responsable du traitement des données») est habilitée à accorder, modifier ou supprimer des droits d'accès.

Des droits d'accès sont accordés aux utilisateurs selon le principe du besoin d'en connaître (lorsque l'accès est strictement nécessaire à l'exécution de leurs tâches) et se limitent à la

finalité de la présente politique en matière de CCTV, ainsi qu'à la maintenance technique du système.

La DG SAFE tient un registre interne des droits d'accès et enregistre systématiquement toute extraction de séquences. L'extraction de séquences pour la maintenance technique est effectuée sans visualisation des images.

## **6.2 Divulcation et transferts**

La DG SAFE peut divulguer ou transférer des séquences du système CCTV aux services de sécurité d'autres institutions européennes ou aux autorités de sécurité, judiciaires ou répressives d'un État membre de l'UE. Ces transferts ne peuvent avoir lieu qu'à la demande de ces parties – aucun transfert régulier ou systématique n'a lieu – et conformément à la procédure décrite dans la présente section<sup>4</sup>.

Toute divulgation ou tout transfert sont soumis à l'approbation de la responsable du traitement des données, à une évaluation rigoureuse de la nécessité de cette divulgation ou de ce transfert, et à l'avis du service juridique du Parlement européen.

Lorsqu'un député au Parlement européen est concerné, l'approbation formelle de la Présidente du Parlement européen est requise. Lorsqu'un membre du personnel est concerné, l'approbation formelle du secrétaire général est requise.

Le délégué à la protection des données du Parlement européen est informé de cette divulgation ou de ce transfert.

La DG SAFE documente le traitement dans son intégralité.

## **7. Durée de conservation**

La DG SAFE conserve les séquences du système CCTV pendant un mois.

Les séquences obtenues dans le cadre d'une enquête de sécurité sont conservées pendant toute sa durée et, le cas échéant, archivées avec l'enquête pour une période maximale de dix ans. La DG SAFE documente rigoureusement cette conservation.

## **8. Mesures de sécurité**

Le Parlement européen recourt aux meilleures solutions technologiques disponibles et respectueuses de la vie privée, conformément aux principes de «respect de la vie privée dès la conception» et de «minimisation des données».

---

<sup>4</sup> La DG SAFE rejette les demandes en vue d'une exploration des données (*data mining*) ou le processus d'analyse des données sous différents angles et de leur synthèse en nouvelles informations utiles.

La DG SAFE s'appuie sur un ensemble de mesures de sécurité techniques et organisationnelles afin de protéger les données contenues dans les séquences du système CCTV.

En tant que tel, le système CCTV n'est connecté à aucun autre système externe au Parlement européen et n'est accessible qu'au personnel spécifiquement autorisé de la DG SAFE. La DG SAFE procède au cryptage des fichiers vidéo archivés pendant la durée de conservation et enregistre scrupuleusement toute manipulation du système.

En outre, la DG SAFE subordonne l'acquisition de droits d'accès à des formations internes et à des engagements en matière de confidentialité à caractère obligatoire.

La DG SAFE procède au floutage systématique des séquences pouvant permettre d'identifier des personnes non concernées par l'enquête de sécurité ou l'enquête auxiliaire.

Les dispositifs nécessaires sont en place pour permettre au système de vidéoprotection du Parlement européen de fonctionner en cas de panne d'alimentation afin de garantir des conditions de sécurité minimales.

## **9. Informations à fournir au public**

Le Parlement européen fournit des informations au public sur le système de vidéoprotection comme suit:

- il publie des avis affichés sur place permettant d'informer le public de la vidéosurveillance et de lui fournir des informations essentielles relatives au traitement de la vidéosurveillance;
- il met à sa disposition un résumé de la politique de vidéoprotection aux comptoirs d'accueil et sur le site web du Parlement européen;
- il met à sa disposition la politique de vidéoprotection sur l'intranet et le site web du Parlement européen.

Pour ces trois modes d'information, une adresse électronique est fournie pour obtenir de plus amples informations sur les droits des personnes concernées.

## **10. Les droits des personnes concernées**

La DG SAFE informe, à titre individuel, toute personne identifiée sur caméra si l'une des conditions suivantes est remplie,

lorsque la DG SAFE:

- conserve leur identité dans un dossier;
- conserve leur identité au-delà de la durée de conservation normale;
- utilise la séquence dans le cadre d'une procédure impliquant la personne concernée;
- divulgue ou transfère des images en dehors de la DG SAFE.

Les citoyens ont le droit de faire valoir leurs droits en matière de protection des données à caractère personnel en vertu du règlement (UE) 2018/1725 en adressant leur demande à la responsable du traitement des données:

**La responsable du traitement des données** de vidéoprotection  
du Parlement européen  
**Directrice générale de la sécurité et de la protection**  
Rue Wiertz 60, B-1047 Bruxelles  
Courriel: [SAFE.dataprotection@europarl.europa.eu](mailto:SAFE.dataprotection@europarl.europa.eu)

La DG SAFE envoie un **accusé de réception** à la personne concernée dans un délai de cinq jours ouvrables à compter de la réception de la demande<sup>5</sup>.

Sur le fond, la DG SAFE **répond à la personne concernée dans un délai de 30 jours calendrier**, sauf si un motif légitime empêche la responsable du traitement des données de respecter le délai. La responsable du traitement des données informe la personne concernée de tout retard éventuel et le motive.

Pour accéder à ses données, la personne concernée doit prouver son identité et, dans la mesure du possible, indiquer la date, l'heure, le lieu et les circonstances de la séquence enregistrée à laquelle elle souhaite accéder, et fournir une photographie récente permettant à la DG SAFE de l'identifier sur les images examinées.

**La responsable du traitement des données peut refuser de donner suite à une demande d'une personne concernée si celle-ci est manifestement non fondée ou excessive**, notamment en raison de son caractère répétitif<sup>6</sup>. La DG SAFE procède dans ce contexte à une évaluation au cas par cas. Il incombe à la responsable du traitement des données de démontrer le caractère manifestement non fondé ou excessif de la demande.

Si la demande est particulièrement complexe ou si elle est susceptible de présenter un risque pour les droits et libertés d'autres personnes concernées, la responsable du traitement des données consultera le délégué à la protection des données du Parlement européen.

Le Parlement européen ne demande pas de contribution financière aux demandeurs dans le cadre de l'exercice de leurs droits en matière de protection des données.

**La responsable du traitement des peut appliquer des limitations aux droits conférés aux personnes concernées** en vertu du règlement (UE) 2018/1725 **lorsque l'exercice de ce droit compromettrait la finalité de l'enquête de sécurité**<sup>7</sup>. La DG SAFE examine cette éventualité au cas par cas et, le cas échéant, documente dûment le traitement et informe le délégué à la protection des données du Parlement européen de toute limitation.

---

<sup>5</sup> Cet accusé de réception n'est pas nécessaire si une réponse sur le fond à la demande est fournie dans le même délai de cinq jours ouvrables. La réponse est envoyée à la personne concernée dans les délais prévus à l'article 14, paragraphe 3, et à l'article 14, paragraphe 4, du règlement (UE) 2018/1725.

<sup>6</sup> Article 14 du règlement (UE) 2018/1725.

<sup>7</sup> Article 25 du règlement (UE) 2018/1725 et annexe I de la décision du Bureau du Parlement européen du 17 juin 2019 sur les modalités d'exécution du règlement (UE) 2018/1725.

## **11. Droit d'introduire une réclamation**

Toute personne a le droit d'introduire une réclamation auprès du Contrôleur européen de la protection des données (adresse électronique: [edps@edps.europa.eu](mailto:edps@edps.europa.eu)) s'il estime que les droits que lui confère le règlement (UE) 2018/1725 sont violés du fait du traitement de ses données à caractère personnel par le Parlement européen. La DG SAFE recommande à toute personne de s'efforcer d'obtenir des informations complémentaires avant d'introduire une réclamation, en contactant:

La **responsable du traitement des données** de vidéoprotection du Parlement européen

**Directrice générale de la sécurité et de la protection**

Rue Wiertz 60, B-1047 Bruxelles

Courriel: [SAFE.dataprotection@europarl.europa.eu](mailto:SAFE.dataprotection@europarl.europa.eu)

et/ou

Le délégué à la protection des données du Parlement européen

Téléphone: +352 4300 23595

Courriel: [data-protection@ep.europa.eu](mailto:data-protection@ep.europa.eu)

Les membres du personnel du Parlement peuvent également s'adresser à leur autorité investie du pouvoir de nomination (AIPN) au titre de l'article 90 du statut.

## **12. Consultations et auto-audit en matière de protection des données**

Le Parlement européen utilise son système de vidéoprotection dans le plein respect du règlement (UE) 2018/1725.

La DG SAFE a consulté le délégué à la protection des données du Parlement européen lors de l'élaboration de cette politique.

La DG SAFE procède à des examens périodiques en matière de protection des données afin de déterminer:

- si elle met correctement en œuvre la politique de vidéoprotection (audit de conformité);
- si le système de vidéoprotection reste indispensable;
- s'il répond toujours à son objectif déclaré;
- s'il n'existe toujours pas de solutions de remplacement adéquates;
- si un exercice de minimisation des données est régulièrement mis en œuvre.