|  |  |  |
| --- | --- | --- |
| **FR**  ***Comité économique et social européen*** |  | C:\Users\mreg\Music\New LOGO CoR\Logo\logo_CoR-vertical-positive-fr-quadri_MR.jpg |

**FR**

**Déclaration de confidentialité – vidéosurveillance**

Le [règlement (UE) 2018/1725](https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R1725&from=FR) s’applique au traitement des données à caractère personnel recueillies à des fins de vidéosurveillance.

Le Comité économique et social européen (CESE) et le Comité européen des régions (CdR) utilisent un système de vidéosurveillance afin d’assurer la sécurité de leurs bâtiments, de leurs biens, de leur personnel et de leurs visiteurs. La présente politique de vidéosurveillance décrit le système de vidéosurveillance des Comités et les garanties prévues par ces derniers afin de protéger les données à caractère personnel, le droit à la vie privée et les autres droits fondamentaux et intérêts légitimes des personnes dont les données personnelles ont été enregistrées par les caméras du système.

1. **Qui est responsable du traitement des données à caractère personnel?**

Les responsables du traitement des données à caractère personnel sont le CESE et le CdR.

Le service compétent est le service de sécurité ([secu@eesc.europa.eu](mailto:secu@eesc.europa.eu)).

1. **Quelle est la finalité du traitement des données?**

Les Comités utilisent leur système de vidéosurveillance aux seules fins de la sécurité et du contrôle d’accès. Le système de vidéosurveillance permet de contrôler l’accès aux bâtiments du CESE et du CdR, et contribue à garantir la sécurité des bâtiments, du personnel et des visiteurs ainsi que celle des biens et des informations présents ou conservés dans les locaux. Il complète les 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 des 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 espaces sécurisés et aux locaux protégés, aux infrastructures informatiques ou aux informations opérationnelles. En outre, la vidéosurveillance permet de prévenir et de détecter le vol de matériel ou de biens détenus par les Comités, les visiteurs ou le personnel, ainsi que les menaces à la sécurité des visiteurs ou du personnel travaillant sur place (telles qu’un incendie ou une agression physique), et de mener des investigations.

Le système n’est utilisé à aucune autre fin. Ainsi, il ne sert pas à surveiller le travail ou la présence du personnel. Les Comités ne recourent pas à la surveillance discrète.

1. **Quelle est la base juridique du traitement des données?**

L’utilisation du système de vidéosurveillance est nécessaire à la gestion et au fonctionnement des Comités [article 5, paragraphe 1, point a) du [règlement (UE) 2018/1725](https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R1725&from=FR)]. Elle s’inscrit dans le cadre des politiques de sécurité plus générales adoptées par les Comités, et plus spécifiquement les *Lignes directrices pour le fonctionnement du service de sécurité*. La politique de vidéosurveillance des Comités a été revue conformément aux recommandations contenues dans les [Lignes directrices du contrôleur européen de la protection des données (CEPD) en matière de vidéosurveillance](https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_fr.pdf) (ci-après les «[lignes directrices](https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_fr.pdf)»).

1. **Quelles sont les données à caractère personnel traitées?**

Les images vidéo enregistrées numériquement.

1. **Qui sont les destinataires ou catégories de destinataires de vos données à caractère personnel?**

Le personnel de sécurité interne et les gardiens de sécurité externes. Seul notre personnel de sécurité interne a accès aux séquences enregistrées. Les images en direct sont également accessibles aux gardiens de sécurité en service, qui travaillent pour une société de sécurité extérieure.

Un accès peut être accordé à la police locale si cela s’avère nécessaire pour enquêter sur des délits ou mener des poursuites. Les images peuvent être transmises à la police locale ou fédérale belge dans le cadre d’enquêtes sur des crimes ou des délits, ou en vue de poursuites. Ces demandes de divulgation doivent être motivées, déposées par écrit auprès du service de sécurité et respecter les exigences de forme et de contenu imposées par la législation nationale en vigueur.

Dans la mesure du possible et indépendamment des obligations imposées au niveau national, les Comités exigeront 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.

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.

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.

1. **Vos données à caractère personnel sont-elles transférées vers un pays tiers (État non membre de l’UE) ou une organisation internationale?**

Vos données à caractère personnel ne seront transmises à aucun État non membre de l’UE ni à aucune organisation internationale.

1. **Comment pouvez-vous exercer vos droits?**

Vous avez le droit de demander l’accès à vos données à caractère personnel. Vous êtes également en droit de demander qu’elles soient modifiées ou supprimées, ou que leur traitement soit soumis à certaines restrictions.

Vous pouvez adresser vos demandes à l’adresse [secu@eesc.europa.eu](mailto:secu@eesc.europa.eu). Toute demande sera traitée dans un délai de 15 jours ouvrables.

Vous avez le droit de saisir le contrôleur européen de la protection des données ([edps@edps.europa.eu](mailto:edps@edps.europa.eu)) si vous estimez que vos droits garantis par le règlement (UE) 2018/1725 ont été violés du fait du traitement de vos données à caractère personnel par les Comités.

1. **Combien de temps vos données à caractère personnel sont-elles conservées?**

Les images sont conservées pendant une période maximale de 30 jours. Toutes les images sont ensuite automatiquement effacées par le système qui écrase les données datant de plus de 30 jours. En l’absence d’incident de sécurité, les enregistrements de manifestants sont effacés dans un délai de 48 heures après la fin de la manifestation.

1. **Les données à caractère personnel collectées sont-elles utilisées pour la prise de décisions automatisée, y compris le profilage?**

Les Comités n’utiliseront pas vos données à caractère personnel pour prendre des décisions automatisées vous concernant. Les «décisions automatisées» sont définies comme des décisions prises sans intervention humaine. Vous avez le droit de refuser le traitement automatisé à tout moment et de réclamer que les décisions soient évaluées par une personne.

1. **Vos données à caractère personnel seront-elles traitées ultérieurement pour une finalité autre que celle pour laquelle elles ont été recueillies?**

Vos données à caractère personnel ne seront pas traitées ultérieurement pour une finalité autre que celle pour laquelle elles ont été recueillies.

1. **Qui pouvez-vous contacter si vous avez des questions à poser ou des réclamations à formuler?**

Si vous avez d’autres questions concernant le traitement de vos données à caractère personnel, veuillez prendre contact avec l’unité chargée de leur traitement ([secu@eesc.europa.eu](mailto:secu@eesc.europa.eu)). Vous pouvez également contacter à tout moment le délégué à la protection des données du CESE ([data.protection@eesc.europa.eu](mailto:data.protection@eesc.europa.eu)), le délégué à la protection des données du CdR (data.protection@cor.europa.eu) et/ou le [contrôleur européen de la protection des données](http://edps.europa.eu/) ([edps@edps.europa.eu](mailto:edps@edps.europa.eu)).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_