Comité économique et social européen

European Committee of the Regions

Bruxelles, le 4 décembre 2017

Politique de vidéosurveillance du Comité européen des régions et du Comité économique et social européen (Information au public)

1. Objet et champ d'application de la politique de vidéosurveillance des Comités

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.

2. Quelle est la base juridique de la vidéosurveillance?

L'utilisation de notre système de vidéosurveillance est nécessaire pour la gestion et le fonctionnement des Comités. Elle s'inscrit dans un ensemble plus large de politiques de sécurité 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 du 17 mars 2010 (ci-après les «lignes directrices»).

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

3.1 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, y compris les agents de sécurité extérieurs.

3.2 **Formation à la protection des données**

Tout nouveau membre du personnel possédant un droit d'accès, y compris les gardiens de sécurité extérieurs (voir le chapitre 8.2 des lignes directrices) reçoivent une formation sur le respect des règles de protection des données. Chaque membre du personnel, y compris le personnel de sécurité externe, signe un accord de confidentialité.

4. **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.

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 des sociétés externes 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.

5. **Comment informons-nous le public?**

5.1 **Avis affichés aux entrées des bâtiments des Comités**

Des avis affichés sur place permettent d'informer le public de la vidéosurveillance et de lui fournir les informations essentielles relatives au traitement des données. Ces avis sont affichés à toutes les entrées des bâtiments des Comités, y compris à l'entrée des garages.

5.2 **Exemplaires disponibles à la réception des bâtiments**

Des exemplaires imprimés de la politique de vidéosurveillance sont également disponibles sur demande à la réception de nos bâtiments et auprès de notre service de sécurité (secu@eesc.europa.eu).

5.3 **Publication sur l'internet**

Le présent document est la version publique de la politique de vidéosurveillance. Il est publié sur l'intranet et les sites internet des Comités.

6. **Pendant combien de temps les données 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.

7. **Comment vérifier, modifier, verrouiller ou supprimer des données à caractère personnel?**

Les membres du public ont le droit d'accéder aux données personnelles les concernant, de les corriger et de les compléter. Toute demande d'accès, de rectification, de verrouillage ou de suppression de données à caractère personnel doit être adressée au service de sécurité (secu@eesc.europa.eu).

À l'heure actuelle, nous ne demandons pas de contribution financière aux personnes qui souhaitent visionner leurs images ou 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 un cas précis soumis à une exemption au titre de l'article 20, paragraphe 1, du règlement nº 45/2001.

8. **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 nº 45/2001 ont été violés du fait du traitement de ses données personnelles par les Comités. Avant d'en arriver là, nous recommandons aux personnes concernées d'essayer d'obtenir satisfaction en contactant:

- le chef du service de sécurité (secu@eesc.europa.eu),
- le délégué à la protection des données concerné:
  - délégué à la protection des données du CdR (data.protection@cor.europa.eu),
  - délégué à la protection des données du CESE (data.protection@eesc.europa.eu).

Les membres du personnel peuvent également saisir l'autorité investie du pouvoir de nomination d'une demande d'évaluation au titre de l'article 90 du statut.