ETAT DE FRIBOURG
STAAT FREIBURG

**Autorité cantonale de la transparence,
de la protection des données et de la médiation**
ATPrDM
**Kantonale Behörde für Öffentlichkeit, Datenschutz
und Mediation** ÖDSMB

La Préposée à la protection des données *a.i.*

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08
www.fr.ch/atprdm

Réf. : MS/nk 2022-LV-6

PRÉAVIS
du 23 décembre 2022

À l'attention de la Préfète de la Sarine, Mme Lise-Marie Graden

Demande d'autorisation d'installation d'un système de vidéosurveillance avec enregistrement
sis à l'Hôtel cantonal, Place de l'Hôtel de Ville 2 et 2a, 1700 Fribourg

Secrétariat général du Grand Conseil, Place de l'Hôtel de Ville 2 et 2a 11, 1700 Fribourg

I. Généralités

Vu

- les articles 12, 24 et 38 de la Constitution du canton de Fribourg du 16 mai 2004 (Cst./FR ; RSF 10.1) ;
- l'article 5 al. 2 de la Loi cantonale du 7 décembre 2010 sur la vidéosurveillance (LVid ; RSF 17.3) ;
- l'article 5 al. 1 de l'Ordonnance cantonale du 23 août 2011 sur la vidéosurveillance (OVid ; RSF 17.31) ;
- la Loi cantonale du 25 novembre 1994 sur la protection des données (LPrD ; RSF 17.1) ;
- le Règlement cantonal du 29 juin 1999 sur la sécurité des données personnelles (RSD ; RSF 17.15) ;
- la Loi cantonale du 4 avril 1972 sur le domaine public (LDP ; RSF 750.1) ;
- la Loi cantonale du 6 septembre 2006 sur le Grand Conseil (LGC ; RSF 121.1),

l'Autorité cantonale de la transparence, de la protection des données et de la médiation (ATPrDM) formule le présent préavis concernant la requête du Secrétariat du Grand Conseil (ci-après : le requérant) visant à l'installation d'un système de vidéosurveillance avec enregistrement, à l'Hôtel cantonal, Place de l'Hôtel de Ville 2 et 2a, 1700 Fribourg, comprenant 4 caméras, dont 1 de type _____ et 3 de type _____, avec possibilité de zoom fonctionnant 24h/24, 7j/7.

Ce préavis se base sur les éléments qui ressortent du formulaire de demande d'autorisation d'installation d'un système de vidéosurveillance avec enregistrement, le Règlement d'utilisation et les annexes transmis par la Préfecture de la Sarine par courrier du 23 mai 2022, les compléments transmis par la Préfecture de la Sarine par courriel du 12 août 2022, les courriels y relatifs ainsi que les mesures provisionnelles de la Préfecture de la Sarine et le préavis de la Ville de Fribourg transmis par courrier du 1er septembre 2022 par la Préfecture de la Sarine.

Le système de vidéosurveillance fait l'objet de ce préavis pour autant que le champ de vision de ses caméras couvre tout ou une partie de lieux publics (art. 2 al. 1 LVid). Sont des lieux publics, les immeubles qui appartiennent au domaine public cantonal ou communal (art. 2 al. 2 let. a LVid). Les immeubles affectés à l'administration public appartiennent au domaine public cantonal (art. 3 al. 1 ch. 1 LDP). Les routes, voies de communication et les places communales appartiennent également au domaine public (art. 3 al. 2 ch. 2 LDP). Au vu des informations fournies par le requérant, les caméras capturent des images de l'intérieur de l'Hôtel cantonal, en particulier de la réception et des couloirs ; ainsi que des images de la Place de l'Hôtel de Ville. Ainsi le présent système de vidéosurveillance entre pleinement dans le champ d'application de la LVid.

Le but du présent préavis est de vérifier la licéité de l'installation du système de vidéosurveillance dont il est question ici. À cette fin, celui-ci donne « les détails techniques ou concrets » sur lesquels il se fonde (TC FR 602 2017 100 à 106 et 111 du 20 janvier 2020, consid. 5.2.). Ainsi les risques sont analysés (*cf.* chap. II), mais également le respect des principes généraux et autres critères légaux, à savoir l'exigence de la base légale, le respect du principe de la proportionnalité, le signalement adéquat du système, le respect du principe de la finalité, la sécurité des données, la durée de conservation des images, l'information aux collaborateurs et collaboratrices, le droit d'accès, le respect de la confidentialité et l'obligation de déclarer les fichiers (*cf.* chap. III, ch. 1 à 10).

II. Analyse des risques

1. Analyse préalable des risques et des mesures de prévention au regard du but poursuivi (art. 3 al. 2 let. e OVid)

Le but du présent système de vidéosurveillance est « de contribuer à garantir à travers la caméra extérieure la sécurité des Députés et du Secrétariat du Grand Conseil en permettant d'observer les rassemblements de personnes et les risques de manifestations désordonnées devant le bâtiment.[…] De contribuer à garantir à travers les caméras intérieures la sécurité des Députés et du Secrétariat du Grand Conseil en permettant d'observer les entrées et sorties dans et depuis la salle du Grand Conseil et des locaux du Secrétariat du Grand Conseil » (cf. art. 1 ch. 3 du Règlement d'utilisation ; ci-après : RU).

Une analyse des risques, à la lumière du principe de la proportionnalité, ne figure pas au dossier. Sur la base des éléments à notre disposition, il peut être déduit ce qui suit :

1.1 Quant à l'analyse des risques

Il s'agit de déterminer s'il peut y avoir des atteintes contre des personnes ou des biens dans les lieux à protéger ou s'il y a un danger concret que des atteintes se produisent. Le dossier ne mentionne aucun dommage. En outre, aucune plainte pénale n'a été portée à la connaissance de l'Autorité.

Le requérant explique agir en prévision de rassemblements de personnes afin d'éviter les risques de manifestations désordonnées devant le bâtiment. Garantir la sécurité des Député-e-s et du Secrétariat du Grand Conseil est recherché. Aucun dommage n'est mentionné.

1.2 Quant aux moyens

Il s'agit de déterminer quels sont les moyens actuels et quels seraient les moyens possibles et moins radicaux que la vidéosurveillance.

Il ressort du dossier que les risques soulevés par le requérant (cf. chap. II, 1.1) sont principalement des risques hypothétiques. Dans cet ordre d'idées, limiter la vidéosurveillance aux sessions du Grand Conseil serait une mesure moins contraignante permettant d'atteindre les objectifs (cf. ég. le préavis de la Ville de Fribourg). Une surveillance par un ou plusieurs agents de sécurité serait une mesure adéquate, notamment lors des sessions du Grand Conseil.

1.3 Quant au but

Comme mentionné au point II. 1.1, le but du présent système de vidéosurveillance est « de contribuer à garantir à travers la caméra extérieure la sécurité des Députés et du Secrétariat du Grand Conseil en permettant d'observer les rassemblements de personnes et les risques de manifestations désordonnées devant le bâtiment.[…] De contribuer à garantir à travers les caméras intérieures la sécurité des Députés et du Secrétariat du Grand Conseil en permettant d'observer les entrées et sorties dans et depuis la salle du Grand Conseil et des locaux du Secrétariat du Grand Conseil » (cf. art. 1 ch. 3 RU).

Aux termes de l'article 3 alinéa 1 LVid, la vidéosurveillance veille à prévenir les atteintes aux personnes et aux biens et contribue à la poursuite et répression des infractions. Ces deux conditions, soit la prévention des atteintes aux biens et/ou aux personnes et la contribution à la poursuite et à la répression d'infractions, sont cumulatives (TC FR 601 2014 46 du 20 août 2015, consid. 3d)).

Les buts mentionnés dans le RU semblent entrer dans le champ d'application de la LVid ; mais, au vu de leur formulation, l'Autorité conseille la reformulation suivante : « de prévenir toute atteinte aux Député-e-s et/ou aux membres du Secrétariat du Grand Conseil lors de session du Grand Conseil et de contribuer à la poursuite et répression des infractions réalisées dans l'enceinte de l'Hôtel cantonal ». Ainsi il paraît envisageable que le moyen projeté permette de remplir les buts poursuivis.

III. Conditions

1. Exigence de la base légale

L'article 38 Cst./FR indique que « toute restriction d'un droit fondamental ou social doit être fondée sur une base légale. Les restrictions graves doivent être prévues par une loi ». Dans cet ordre d'idées, selon l'article 4 LPrD, le traitement de données personnelles ne peut se faire que si une disposition légale le prévoit.

Ainsi les traitements de données personnelles qu'implique la vidéosurveillance ainsi que les éventuelles restrictions qu'elle engendre sont régis par la LVid.

2. Respect du principe de la proportionnalité (art. 4 al. 1 let. a LVid)

L'article 4 LVid prévoit que les systèmes de vidéosurveillance avec enregistrement sont soumis au respect du principe de la proportionnalité (let. a).

La vidéosurveillance porte atteinte à plusieurs libertés (not. art. 11 al. 2 Cst./FR ; art. 12 al. 1 Cst./FR et art. 8 CEDH ; art. 12 al. 2 Cst./FR : cf. FLÜCKIGER/AUER, La vidéosurveillance dans l'œil de la Constitution fédérale, AJP/PJA 2006, p. 931).

La surveillance doit être adéquate ; c'est-à-dire apte à atteindre le but visé et limitée à ce qui est nécessaire. La surveillance au moyen d'enregistrements vidéo permet la constatation d'infractions en assurant la conservation des preuves et en permettant ainsi un taux d'élucidation élevé. Grâce à l'effet

dissuasif qui y est lié, les infractions sont combattues dans un but de maintien de la sécurité et de l'ordre public (TC FR 601 2014 46 du 20 août 2015, consid. 2b/cc). Pour être proportionnée, la vidéosurveillance ne peut être installée qu'aux endroits où elle s'avère nécessaire (FLÜCKIGER/AUER, op. cit., p. 938). Le principe de la proportionnalité s'oppose à une vidéosurveillance généralisée de tout le territoire sans tenir compte du niveau d'insécurité qui y règne (FLÜCKIGER/AUER, op. cit., p. 938). En l'espèce, l'installation des caméras aux entrées et sorties est apte à limiter les atteintes aux personnes et aux biens et peut comporter un effet dissuasif.

Le principe de la proportionnalité ne s'applique pas seulement à la surveillance elle-même, mais également au dispositif technique choisi (Message n° 202 du Conseil d'Etat du 6 juillet 2010 accompagnant le projet de loi sur la vidéosurveillance, *in* BGC novembre 2010 1967, p. 1969). Selon les informations communiquées, la transmission est réalisée par câbles. L'enregistrement ainsi que la vision en direct sont envisagés (présence d'écran pour les huissiers et le Secrétariat). Or, pour que le présent système soit conforme au principe de la proportionnalité, une vidéosurveillance avec enregistrement simple, dont l'enregistrement est effacé automatiquement après une durée qui n'est pas doublé d'un suivi en temps réel et est visionné et utilisé uniquement en cas de délits avérés, est largement suffisante pour les caméras sur le domaine public (place et lieux de passage). Selon la jurisprudence et les recommandations du Préposé fédéral à la protection des données et à la transparence[1], le dispositif technique utilisé doit également respecter le principe de proportionnalité, notamment en préservant l'anonymat des personnes. En l'occurrence, un système de floutage des images ou des bandes noires doit être employé afin de réduire au maximum l'atteinte aux libertés des personnes filmées, de sorte que l'installation ne doit filmer que les parties absolument nécessaires (cf. commentaires ci-dessous par caméra). En cas d'infractions avérées, les floutages peuvent être ponctuellement désactivés afin de dévoiler l'identité du responsable (cf. Arrêt TC FR 601 2014 46, consid. 3b). L'efficacité des systèmes de vidéosurveillance n'est ainsi aucunement réduite.

Le requérant est doté d'écrans pour la Secrétaire ou le Secrétaire général-e du Grand Conseil et l'Huissier ou l'Huissière. Il importe de préciser le nombre d'écran et les lieux d'installation. Pour être conforme à la protection des données, il s'agira de disposer l'écran afin qu'aucune personne non autorisée ne puisse accéder aux images.

Sous l'angle de la nécessité, d'autres mesures moins incisives seraient envisageables afin d'atteindre le même but de prévention et de répression des atteintes aux biens et aux personnes (*cf.* chap. II, ch. 1.2).

La base légale doit être suffisamment précise pour que le citoyen puisse adapter son comportement et mesurer la conséquence d'un tel comportement avec une certaine certitude. […]Il sied de rappeler que les installations situées dans des lieux de passages fréquents portent de plus grandes atteintes aux libertés des personnes qu'une surveillance dans un endroit à l'écart (TC FR 601 2014 46, consid. 3b) cc et réf.). Le site concerné par la présente demande d'autorisation sont proches de routes. Il s'agit de lieux de passage (voire proches de passages). Dans cette compréhension, la vision en temps réel ne passe pas l'examen de la proportionnalité. L'intérêt à observer les rassemblements de personne en raison de risques de manifestations désordonnées ne l'emporte pas sur l'atteinte importante au droit de la personnalité des personnes concernées.

---

[1] https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/technologien/videoueberwachung/explications-sur-la-videosurveillance-dans-les-vestiaires-et-dan.html).

Afin d'avoir une vue générale, chaque caméra est analysée à la lumière du principe de la proportionnalité. L'appréciation est réalisée d'après les champs de vision transmis ; c'est-à-dire les images figurant au dossier. Afin de simplifier la lecture, nous abordons les caméras dans l'ordre croissant :

- **Caméra 1 – Extérieur – enregistrement des images et vision en temps réel 24h/24.** La vision en temps réel ne respecte pas le principe de la proportionnalité. L'enregistrement des images est admis ;

- **Caméra 2 – Intérieur 1 couloir 1er étage – enregistrement des images et vision en temps réel 24h/24.** Il ressort du dossier que la volonté soit d'éviter les débordements lors de rassemblement et d'assurer la sécurité des membres et collaborateurs et collaboratrices du Grand Conseil. La vision en temps réel ne respecte pas le principe de la proportionnalité. L'enregistrement des images est admis ;

- **Caméra 3 – Intérieur 2 couloir 1er étage – enregistrement des images et vision en temps réel 24h/24.** Il est renvoyé à l'argumentation de la caméra 2 ;

- **Caméra 4 – Intérieur SGC 2ème étage – enregistrement des images et vision en temps réel 24h/24.** Il est renvoyé à l'argumentation de la caméra 2 ;

La question de la proportionnalité de l'horaire de fonctionnement se pose pour toutes les caméras prévues. La vision en temps réel et l'enregistrement des images sont prévus en continu (24h/24 et 7j/7). Dès lors que la vision en direct dépend de la présence de la Secrétaire ou du Secrétaire général-e du Grand Conseil et de l'Huissier ou de l'Huissière, un horaire de bureau doit être favorisé, respectivement les sessions du Grand conseil ou le déroulement d'autres évènements pertinents. En effet, les extérieurs filmés servent aussi de place de marché hebdomadaire, et divers marchand-e-s, artisan-e-s, citoyen-ne-s peuvent s'y trouver, qu'il n'y a pas lieu de filmer. La vision en direct en sus de l'enregistrement porte une atteinte grave à la personnalité. Puisque selon les informations du dossier, la caméra filme l'extérieur du bâtiment, il semble suffisant de limiter cet enregistrement aux heures de bureau, respectivement aux dates de sessions du Grand Conseil ou lors du déroulement d'autres évènements pertinents. Des informations complémentaires sont nécessaires pour apprécier la proportionnalité et l'intérêt public soulevé. L'horaire choisit est renseigné. Le RU est modifié en ce sens.

Dès lors que la surveillance concerne la surveillance de rassemblement, il importe de mentionner que la reconnaissance faciale n'est pas autorisée, conformément au principe de la proportionnalité. Il s'agit d'un système d'intelligence artificielle portant une atteinte grave à la personnalité.

3. Signalement adéquat du système (art. 4 al. 1 let. b LVid)

Le système doit être signalé à ses abords de manière adéquate (art. 4 al. 1 let. b LVid). Partant, le RU est complété de la manière suivante : « le système de vidéosurveillance est signalé à ses abords au moyen de panneaux informant sans équivoque les personnes se trouvant dans la zone surveillée (p. ex. sous la forme d'un pictogramme) et mentionnant le responsable du système ». Le requérant signale la vidéosurveillance sur le « Totem ». Dès lors que la place de l'Hôtel de Ville est sous vidéosurveillance, la signalisation doit être placée avant que toute personne n'entre dans le champ de vision des caméras. Ainsi les personnes concernées peuvent se déterminer en connaissance de cause.

4. Respect du principe de la finalité (art. 4 al. 1 let. c LVid)

La finalité paraît en adéquation avec l'exigence légale (art. 1 ch. 3 RU), sous réserve du chap. II, ch. 1.3.

5. Sécurité des données (art. 4 al. 1 let. d LVid)

L'organe responsable du système de vidéosurveillance est l'organe dirigeant (art. 2 OVid), c'est-à-dire la Bureau (art. 4 al. 1 LGC). Nous conseillons de modifier le RU en ce sens.

Le nombre des personnes autorisées à avoir accès est limité. Le Président du Grand conseil a un accès selon l'article 5 chiffre 3 RU, mais ne figure pas dans la liste des personnes autorisées. Le RU devrait être corrigé sur ce point. Il importe de distinguer les différentes autorisations ainsi que les droits d'accès y relatifs selon les fonctions et les rôles des personnes (accès aux enregistrements, autorisation d'extraction, accès au serveur, accès aux images en direct, etc.) (cf. art. 5 ch. 3 RU). Les titulaires d'autorisation personnelle (art. 2, ch. 2, RU) consultent les images enregistrées qu'en cas de nécessité, à savoir en cas d'atteinte avérée. La double authentification pour l'accès est conseillée.

Il ressort du dossier que les écrans sont à la disposition de la Secrétaire ou du Secrétaire général-e du Grand Conseil et de l'Huissier ou de l'Huissière. Seuls ceux-ci ont accès aux images en direct. Les écrans de visualisation sont placés et orientés de manière à ce qu'aucune personne non autorisée n'ait accès aux images (par exemple : face à un mur). Il importe de préciser le nombre d'écran et les lieux d'installation. Nous conseillons de modifier le RU en ce sens.

Le RU doit mentionner que l'enregistrement des images est prévu aux horaires de bureau, respectivement lors des sessions du Grand conseil ou lors du déroulement d'autres évènements pertinents. En cas d'atteinte, l'image est « extraite » en attente de la demande du juge (enregistrement sur support à part). L'article 4 RU est complété d'un chiffre distinguant les enregistrements continus standard des enregistrements faisant suite à une extraction de données ; d'un chiffre expliquant que les images sont uniquement enregistrées (voire visionnées en direct : sous réserve de l'appréciation de la Préfecture) ; et d'un chiffre expliquant que toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons, voire permettant la reconnaissance faciale, n'est pas autorisée.

Concernant la sécurité des données, les informations relatives au fournisseur ou à l'entreprise d'installation et les mesures techniques (tels que le chiffrement du transfert et du stockage des données, le détenteur des clés, le contrat y relatif) doivent faire l'objet d'une analyse spécifique. En cas de sous-traitance, les articles 18 et 12*b* ss LPrD doivent être respectés.

Nous conseillons de prévoir une information dans le RU quant à la limitation de l'accès au serveur local ainsi qu'au local où sont stockés les enregistrements et/ou extractions aux seules personnes autorisées (*cf.* art. 2, ch. 2, RU).

6. Durée de conservation des images (art. 4 al. 1 let. e LVid)

A moins qu'elles ne soient conservées dans le cadre d'une procédure, les données enregistrées doivent être détruites après 30 jours ou, en cas d'atteinte aux personnes ou aux biens, après 100 jours au maximum. Dans tous les cas, nous conseillons d'effectuer une analyse pour déterminer si les données peuvent être détruites après un délai plus court que les 30 jours prévus par la loi. En raison de la jurisprudence du Tribunal fédéral (cf. ATF 133 I 77, JdT 2007 I 591) et des recommandations du

Préposé fédéral à la protection des données et à la transparence[2], notre Autorité conseille une destruction automatique après 10 jours. Les infractions contre les biens étant constatées par les autorités étatiques elle-même (et non sur plainte) une longue durée de conservation ne nous semble pas indispensable en cas d'atteinte.

En cas d'atteinte avérée aux personnes ou aux biens, les données enregistrées sont extraites sur un support informatique et sont détruites après 100 jours au maximum. Un protocole de destruction est conservé. Les responsables doivent s'informer régulièrement de toute situation pouvant entrer dans le but de la protection. Le RU devrait préciser ces aspects.

7. Informations aux collaboratrices et collaborateurs

Le requérant est rendu attentif au fait que, dans la mesure où il filme ses employé-e-s, ces derniers doivent être informés des endroits sous vidéosurveillance et des horaires où le système fonctionne.

8. Droit d'accès (art. 1 al. 2 in fine LVid ; art. 23 LPrD)

Un article relatif au droit d'accès devrait être ajouté dans le RU. Celui-ci précise ainsi que « toute personne peut demander au responsable du système l'accès à ses propres données. Le responsable du système répond à la demande tout en respectant les droits de la personnalité des autres personnes concernées (en les floutant par exemple) ».

9. Clause de confidentialité

Le prestataire mandaté ainsi que ses collaboratrices et collaborateurs doivent signer une clause de confidentialité, réservant des suites juridiques en cas de non-respect, dans la mesure où il s'agit de données sensibles et soumises au secret de fonction.

En effet, quand bien même le secret de fonction s'applique aux fonctionnaires, la notion d'auxiliaire, qui comprend non seulement la personne effectivement apte à remplir la mission confiée et qui l'accepte ainsi que toutes celles qui participent effectivement à l'accomplissement de la tâche liée à l'exécution du mandat ou du contrat, s'applique par analogie à l'article 320 du Code pénal suisse (concernant le secret de fonction). Le secret de fonction[3] étant applicable à l'auxiliaire, le contrat de service ou de mandat se doit de préciser cela (*cf.* MÉTILLE, L'utilisation de l'informatique en nuage par l'administration publique, AJP/PJA 6/2019, p. 609 ss, p. 613 s.). Nous conseillons de prévoir que la clause de confidentialité soit annexée au RU (art. 7 RU).

10. Déclaration de fichier

Conformément aux articles 19 ss LPrD, les fichiers doivent être déclarés à l'ATPrDM avant leur ouverture.

---

[2] (cf. https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/technologien/videoueberwachung/explications-sur-la-videosurveillance-sur-le-lieu-de-travail.html)

[3] À ce sujet, voir également : (*cf.* BO CN 22.7249 Keller-Sutter Karin, L'usage d'un service de cloud à l'étranger par une entité soumise à l'art. 320 CP constitue-t-elle une violation du secret de fonction ?).

IV. Conclusion

Dans le cadre de la demande d'installation du système de vidéosurveillance avec enregistrement sis à **l'Hôtel cantonal**, Place de l'Hôtel de Ville 2 et 2a, 1700 Fribourg

par

le Secrétariat général du Grand Conseil, Place de l'Hôtel de Ville 2 et 2a, 1700 Fribourg

l'Autorité cantonale de la transparence, de la protection des données et de la médiation émet un :

- **partiellement favorable** à la demande d'installation, avec enregistrement, de la **caméra 1.** En effet, nous préavisons défavorablement la vision en temps réel ;
- **partiellement favorable** à la demande d'installation des caméras **n° 2 à n° 4** avec enregistrement ;

aux conditions suivantes :

a. analyse des risques : l'organe responsable peut réévaluer le système de vidéosurveillance, la situation, les risques et les moyens dans un délai de trois ans.

b. proportionnalité : Des informations complémentaires sont fournies à la Préfecture concernant le besoin et la nécessité d'installer les caméras 2 à 4 (cf. ci-dessus, notamment la vision en direct) pour une appréciation définitive. Le nombre de caméra est adapté. Le RU est modifié en ce sens.

Concernant la vision en direct des caméras 2 à 4, un horaire restreint est favorisé, voire limité à l'horaire de présence de la Secrétaire ou du Secrétaire général-e du Grand Conseil, respectivement de l'Huissier ou de l'Huissière ou d'autres évènements particuliers. L'horaire restreint est renseigné à la Préfecture. Le RU est modifié en ce sens. Pour la caméra 1, la proportionnalité de l'horaire de fonctionnement de l'enregistrement est également analysée.

La surveillance en extérieur nécessite la présence d'un système de masquage de zone (cache ou bloque noir) en présence d'habitations privées ou véhicules (plaque d'immatriculation) dans le champ de vision.

c. sécurité des données : L'article 2 chiffre 1 RU précise que le responsable du système est le Bureau.

Le nombre de personnes autorisées est limité. Les accès et autorisations sont distinguées selon les fonctions et les rôles des personnes et sont conformes à la liste de l'article 2 RU (exemple de l'art. 5 ch. 3 RU). Le RU est modifié en ce sens.

Le RU précise que les titulaires d'autorisation consultent les images qu'en cas d'atteinte avérée.

Sous réserve de l'appréciation de la Préfecture (vision en direct), le nombre d'écran et leur localisation sont renseignés. Ils sont placés de manière à ce que les personnes non autorisées ne puissent y avoir accès (exemple : face au mur).

Le RU mentionne que l'enregistrement des images fonctionne pendant les heures de bureau, les sessions du Grand Conseil ou d'autres évènements particuliers, sur détection de mouvement. Les utilisateurs changent régulièrement leurs mots de passe. Ainsi une double authentification est recommandée.

L'article 4 RU est complété d'un chiffre distinguant les enregistrements continus standard des enregistrements faisant suite à une extraction de données ; d'un chiffre expliquant que les images sont uniquement enregistrées (voire visionnées en direct : sous réserve de l'appréciation de la Préfecture) ; et d'un chiffre expliquant que toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons, voire permettant la reconnaissance faciale, n'est pas autorisée.

La sous-traitance demande le respect des 12*b* ss LPrD. L'article 2 chiffre 2 2ème paragraphe RU est adapté. La limitation de l'accès au serveur local ainsi qu'au local où sont stockés les enregistrements et/ou extractions aux seules personnes autorisées (cf. art. 2, ch. 2, RU) est spécifiée dans le RU. La Préfecture est renseignée à ce sujet ainsi qu'en ce qui concerne la localisation du serveur local.

Les images enregistrées et celles extraites sont stockées sur un support physique indépendant.

d. *signalement* : un chiffre est ajouté à l'article 1 RU avec la formulation suivante : « le système de vidéosurveillance est signalé à ses abords au moyen de panneaux informant sans équivoque les personnes se trouvant dans la zone surveillée (p. ex. sous la forme d'un pictogramme) et mentionnant le responsable du système ».

e. *finalité des* données : le but de l'installation mentionné à l'article 1 chiffre 3 RU est modifié de la manière suivante : « de prévenir toute atteinte aux Débuté-e-s et/ou aux membres du Secrétariat du Grand Conseil lors des sessions du Grand Conseil et de contribuer à la poursuite et répression des infractions réalisées dans l'enceinte de l'Hôtel cantonal ».

f. *destruction des images* : l'article 4 chiffre 3 RU doit déclarer qu'il incombe aux responsables de s'informer régulièrement de la situation.

Comme le mentionne le RU, les données enregistrées doivent être détruites automatiquement au maximum après 30 jours. En cas d'atteintes avérées aux personnes et aux biens, les enregistrements (extraction) peuvent être conservées jusqu'à 100 jours.

g. *informations aux collaboratrices et collaborateurs :* les collaboratrices et collaborateurs doivent être informés des endroits sous vidéosurveillance et des horaires où le système fonctionne.

h. *droit d'accès :* le RU est complété d'un article relatif au droit d'accès de toute personne souhaitant consulter ses propres données.

i. *clause de confidentialité :* le prestataire mandaté ainsi que ses collaboratrices et collaborateurs signent une clause de confidentialité.

j. *obligation de déclarer le fichier* : les fichiers doivent être déclarés à l'ATPrDM avant leur ouverture, conformément aux articles 19 ss LPrD.

V. Remarques

> Les dispositions légales pertinentes doivent être respectées, notamment celles en matière de protection des données. Les données qui sont accessibles à la requérante ne doivent être consultées que dans le but pour lequel l'autorisation de l'installation de vidéosurveillance a été demandée.

> Toute modification de l'installation et/ou de son but devra être annoncée et notre Autorité se réserve le droit de modifier son préavis (art. 5 al. 3 OVid).

> L'article 30*a* alinéa 1 lettre c LPrD est réservé.

> Le présent préavis peut être publié.

Martine Stoffel
Préposée cantonale à la transparence
Préposée cantonale à la protection des données *a.i.*

Annexes
—
- dossier en retour
- formulaire de demande