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 cantonale à la protection des données

Rue des Chanoines 2, 1700 Fribourg

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

Réf. : FH/nk 2021-LV-32

PRÉAVIS
du 11 août 2022

À l'attention du Préfet de la Broye, M. Nicolas Kilchoer

Demande d'autorisation d'installation d'un système de vidéosurveillance avec enregistrement
sis au Musée communal « Des Grenouilles », à la Rue du Musée 13, 1470 Estavayer-le-Lac

Commune d'Estavayer, Rue de l'Hôtel de Ville 11, 1470 Estavayer-le-lac

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 25 septembre 1980 sur les communes (LCo ; RSF 140.1) ;
- le Règlement cantonale du 28 décembre 1981 d'exécution de la Loi sur les communes (RELCo ; 140.11) ;
- la Loi cantonale du 4 avril 1972 sur le domaine public (LDP ; RSF 750.1),

l'Autorité cantonale de la transparence, de la protection des données et de la médiation (ATPrDM) formule le présent préavis concernant la requête de la commune d'Estavayer (ci-après : la requérante) visant à l'installation d'un système de vidéosurveillance avec enregistrement, au Musée communal « Des Grenouilles », sis à la Rue du Musée 13, 1470 Estavayer-le-Lac, comprenant 6 caméras _____, avec possibilité de zoom, reconnaissance faciale, fonctionnant 24h/24, 7j/7 sur détection de mouvement.

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 Broye par courrier du 6 décembre 2021 ainsi que les compléments transmis par la Préfecture de la Broye par courriel du 4 mai 2022.

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 (cf. art. 2 al. 2 let. a LVid). Au vu des informations fournies par la requérante, les caméras capturent des images de l'intérieur du Musée, en particulier de la réception, de la salle des tableaux, de la cuisine, de la salle des oiseaux et de la salle des grenouilles. 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 protéger tous les objets d'art, armes et grenouilles naturalisées et sauvegarder efficacement le patrimoine staviacois et permettra d'observer de manière efficace toutes les salles du Musée » (cf. art. 1 ch. 3 du Règlement d'utilisation ; ci-après : RU) ainsi que de surveiller et protéger de manière continue les objets exposés dans le Musée communal, identifier les personnes malveillantes en cas de détériorations ou de vols et transmettre les séquences d'enregistrements à l'autorité cantonale (Police cantonale – Ministère Public) en cas de délits constaté (*cf*. formulaire de demande du 5 novembre 2021).

Une analyse des risques, à la lumière du principe de la proportionnalité, figure 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 mentionne que ces dernières années de nombreux vols d'objets d'art ont été commis dans les diverses salle du Musée.

Concernant les vols annoncés, il sied de relever que des précisions font défaut, notamment le nombre de vols, les salles et lieux concernés, les dates et la fréquence ainsi que le montant des dommages. En outre, aucune plainte pénale n'a été portée à la connaissance de l'Autorité.

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 cinq employés sont, à tour de rôle, présents pendant les heures d'ouverture du Musée communal et ont accès en temps réel aux images de vidéosurveillance. Un éclairage adéquat a été mis en place dans les différentes salles.

Une surveillance par un ou plusieurs agents de sécurité serait une mesure adéquate. La requérante n'apporte cependant aucune précision quant aux raisons propres à l'installation de la vidéosurveillance plutôt qu'à la présence d'agents de sécurité. En outre, la requérante n'apporte aucune information au sujet du système de sécurité, notamment les bienfaits, voire la portée des mesures. Au vu des objets de valeur conservée dans le Musée, un système doit avoir été mis en place.

1.3 Quant au but

Comme mentionné au point II. 1.1, le but du présent système de vidéosurveillance est « de protéger tous les objets d'art, armes et grenouilles naturalisées et sauvegarder efficacement le patrimoine staviacois et permettra d'observer de manière efficace toutes les salles du Musée » (cf. art. 1 ch. 3 RU) ainsi que de surveiller et protéger de manière continue les objets exposés dans le Musée communal, identifier les personnes malveillantes en cas de détériorations ou de vols et transmettre les séquences d'enregistrements à l'autorité cantonale (Police cantonale – Ministère Public) en cas de délits constaté (*cf*. formulaire de demande du 5 novembre 2021).

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 et des buts énoncés dans le formulaire de demande d'autorisation, l'Autorité conseille vivement la reformulation suivante : « protéger tous les objets d'art, armes et grenouilles naturalisées, sauvegarder efficacement le patrimoine staviacois et contribuer à la poursuite et répression des infractions réalisées dans les salles du Musée ». 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 déclare 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 : la liberté personnelle, et plus particulièrement la triple garantie de l'intégrité physique et psychique et de la liberté de mouvement (art. 11 al. 2 Cst./FR), le droit au respect de la sphère privée (art. 12 al. 1 Cst./FR et 8 CEDH), le droit d'être protégé contre l'emploi abusif des données personnelles (art. 12 al. 2 Cst./FR) et la liberté de réunion (art. 24 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, c'est-à-dire dans les lieux où l'intérêt public visé ne parvient pas à être atteint par d'autres moyens (FLÜCKIGER/AUER, op. cit., p. 938). Concrètement, la vidéosurveillance doit se limiter aux endroits où, selon l'expérience, se déroulent plus fréquemment des actes de vandalisme et dans lesquels règne par conséquent un plus grand sentiment d'insécurité. 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 à la réception, à la salle des tableaux, à la cuisine, à la salle des oiseaux et à la salle des grenouilles 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). L'atteinte est grave si la vidéosurveillance est doublée d'un traitement informatisé permettant de suivre automatiquement une scène, d'initier des alarmes en fonction de l'analyse de comportement types ou de caractéristiques prédéfinis. Le recours à Internet pour le transit des données, leur visualisation ou le pilotage des caméras augmente l'atteinte potentielle, en particulier en l'absence d'un système de cryptage permettant aisément de diffuser ces données sans restriction (FLÜCKIGER/AUER, op. cit., p. 934). Selon les informations communiquées, la reconnaissance faciale est possible et l'enregistrement ainsi que la vision en direct sont envisagés. 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 brève durée doublé d'un suivi en temps réel pendant les horaires d'ouverture, visionné et utilisé uniquement en cas de délits avérés, est largement suffisante dans le cas d'espèce. 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. La requérante est dotée d'un écran à la réception. 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).

Au sens de la proportionnalité au sens étroit, l'intérêt public à la prévention et à la répression d'infractions (dégâts matériels, atteintes à la personne) doit primer l'intérêt privé au respect des libertés personnelles des personnes (TC FR 601 2014 46, consid. 2b/cc et réf. citées). Pour que l'atteinte aux

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

libertés ne soit pas disproportionnée, il est indispensable de veiller à la mise en place de mesures techniques.

Afin d'avoir une vue générale, chaque caméra est analysée à la lumière du principe de la proportionnalité, sous réserve des champs de vision définitifs. Il est relevé que 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 – réception, salle des armes – enregistrement des images et vision en temps réel 24h/24.** La caméra respecte le principe de la proportionnalité. La vision en temps réel ne respecte pas le principe de la proportionnalité ;

- **Caméra 2 – salle des tableaux – enregistrement des images et vision en temps réel 24h/24.** La caméra respecte le principe de la proportionnalité. La vision en temps réel ne respecte pas le principe de la proportionnalité ;

- **Caméra 3 – salle des tableaux bis – enregistrement des images et vision en temps réel 24h/24.** La caméra respecte le principe de la proportionnalité. La vision en temps réel ne respecte pas le principe de la proportionnalité ;

- **Caméra 4 – cuisine – enregistrement des images et vision en temps réel 24h/24.** La caméra respecte le principe de la proportionnalité. La vision en temps réel ne respecte pas le principe de la proportionnalité ;

- **Caméra 5 – salle des oiseaux – enregistrement des images et vision en temps réel 24h/24.** La caméra respecte le principe de la proportionnalité. La vision en temps réel ne respecte pas le principe de la proportionnalité ;

- **Caméra 6 – salle des grenouilles – enregistrement des images et vision en temps réel 24h/24.** La caméra respecte le principe de la proportionnalité. La vision en temps réel ne respecte pas le principe de la proportionnalité ;

La question de la proportionnalité de l'horaire de fonctionnement se pose. La vision en temps réel est prévue en continue (24h/24 et 7j/7). Dès lors que la vision en direct dépend de la présence de collaborateurs ou collaboratrice, l'horaire de présence de ceux-ci ou celles-ci doit être renseigné. Selon les informations communiquées, l'horaire d'ouverture est de mars à décembre, mardi au dimanche, de 13h à 18h. La volonté étant de surveillée les visiteurs, l'horaire d'ouverture du musée doit être privilégié. Le RU est modifié en ce sens et l'horaire lui est annexé.

L'article 1 chiffre 4 RU précise que le système fonctionne 24h/24, 7j/7 et en continu, avec détection de mouvement. Conformément au principe de la proportionnalité, l'enregistrement des images doit être enclenché suite à la détection de mouvement. Le RU est précisé en ce sens.

Il ressort du dossier qu'un écran est installé à la réception. L'article 2, chiffre 2, RU mentionne cinq personnes autorisées à visionner les images en temps réel. Pourtant, l'article 4, chiffre 2, RU déclare que « les images enregistrées *ne sont pas* visionnées en temps réel, mais en dehors de la plage d'ouverture horaire du musée et par les 2 personnes habilitées à cet effet ». Seuls les collaborateurs et les collaboratrices de la réception 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). Le RU est modifié en ce sens et le tableau annexé complété.

S'agissant d'un système d'intelligence artificielle portant une atteinte grave à la personnalité, la reconnaissance faciale n'est pas autorisée, conformément au principe de la proportionnalité. En outre, une base légale serait nécessaire pour permettre une interconnexion avec d'autres bases de données.

Une réévaluation peut être opérée dans un délai de trois ans concernant notamment les risques d'atteinte et la portée de la mesure.

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 ».

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

La finalité paraît en adéquation avec l'exigence légale (art. 4 ch. 1 RU), sous réserve du chap. II, ch. 1.3.

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

Le Conseil communal est l'organe responsable du système de vidéosurveillance conformément à l'article 2 alinéa 1 lettre c OVid. L'article 2 chiffre 1 RU est modifié en ce sens.

Les titulaires d'autorisation personnelle (art. 2, ch. 2, RU ; autorisation enregistrement) consultent les images enregistrées qu'en cas de nécessité, à savoir en cas d'atteinte avérée. L'autorisation ainsi que les droits d'accès y relatifs doivent être distingués selon les fonctions et les rôles des personnes (accès aux enregistrements, autorisation d'extraction, accès au serveur, etc.). Ces éléments doivent figurer dans le RU (art. 5).

Comme expliqué, l'article 1 chiffre 4 RU parle d'un fonctionnement 24h/24, 7j/7 en continu, avec détection de mouvement. Le RU doit ainsi être précisé. L'article 4 RU est complété d'un chiffre expliquant que les images sont enregistrées sur détection de mouvement. L'article 4 chiffre 9 précise que toute fonctionnalité permettant la reconnaissance faciale n'est pas autorisée.

Concernant la sécurité des données, les informations relatives au fournisseur ou à l'entreprise d'installation (si externalisation) et les mesures techniques (tels que le chiffrement du transfert et du stockage des données, le détenteur des clés, le contrat y relatif) font défaut et devront faire l'objet d'une analyse spécifique. En cas de sous-traitance, les articles 18 et 12*b* ss LPrD doivent être respectés. En effet, lorsque l'organe public fait traiter des données par une entreprise externe, des conditions plus strictes doivent être appliquées et doivent être réglées dans un contrat (art. 18 LPrD). Le contrat doit notamment contenir une garantie du niveau adéquat de protection des données ; le lieu du traitement des enregistrements doit être connu et sécurisé ; la durée du contrat ainsi que la durée de conservation des enregistrements doit être fixée ; les modalités de transfert des données du mandataire à la requérante doivent être mises en place ; les responsabilités entre le mandataire et le sous-traitant doivent être réparties ; les modalités selon lesquelles les enregistrements sont sauvegardés, archivés et détruits doivent être décrites avec précision ; des contrôles doivent pourvoir être effectués par la requérante, la Préfecture ainsi que par l'ATPrDM, sur les activités du mandataire sous-traitant ; le for de la poursuite ainsi que le droit applicable sont suisses. En outre, les enregistrements doivent être chiffrés au niveau de la transmission et du stockage. La clé de cryptage doit être uniquement détenu par l'organe public.

En effet, le mandataire ne doit pas pouvoir avoir accès aux données. Le RU prévoit que la maintenance ne pourra pas être effectuée à distance.

Des précisions doivent être fournies concernant le serveur local. Une information est faite 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 ; autorisation enregistrement). L'hébergement des données est local, sans accès à distance. Le RU est modifié en ce sens.

Il ressort des aspects techniques dans le dossier que le système (notamment le serveur local) fonctionne avec Internet. L'article 5 chiffre 4 RU mentionne que « les images enregistrées et celles extraites doivent être stockées sur un support physique indépendant, sans accès à distance (réseau sans fils ou internet) ». Ainsi aucun réseau sans fils, interconnexion ni Internet n'est utilisé-e.

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

Les responsables doivent s'informer régulièrement de toute situation pouvant entrer dans le but de la protection. Les durées de conservation sont conformes à la législation (*cf.* art. 4 ch. 5 RU).

7. Informations aux collaboratrices et collaborateurs

La requérante est rendue attentive au fait que, dans la mesure où elle 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)

Le RU prévoit un droit d'accès (art. 6 RU).

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[2] 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.). Le RU prévoit que la clause de confidentialité est 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] 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 au **Musée communal « Des Grenouilles »**, à la Rue du Musée 13, 1470 Estavayer-le-Lac

par

la commune d'Estavayer, Rue de l'Hôtel de Ville 11, 1470 Estavayer-le-Lac

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

- préavis **favorable** à la demande d'installation, avec enregistrement et vision en temps réel, des **caméras 1 à 6** ;

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 : la vision en temps réel est limité à l'horaire d'ouverture du Musée. L'horaire est annexée au RU. L'écran de la réception est placé de sorte que les personne non autorisées ne puissent avoir accès aux images. Le RU est modifié en ce sens.

c. 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 ».

d. sécurité des données : L'article 2 chiffre 1 RU précise que le responsable du traitement est le Conseil communal.

l'article 4 RU est complété d'un chiffre expliquant que les images sont enregistrées sur détection de mouvement ; d'un chiffre déclarant que les images sont visionnées en temps réel, selon l'horaire annexé ; d'un chiffre expliquant que toute fonctionnalité permettant la reconnaissance faciale n'est pas autorisée.

En cas de sous-traitance et pour être conforme aux exigences des art. 18 et 12*b* al. 1 let. b LPrD, un contrat particulier doit être conclu. Les autorisations d'accès doivent spécifiquement être distinguées selon l'accès aux enregistrements, l'accès aux images en direct et les autres types d'autorisation. L'article 2 chiffre 2 RU est modifié en ce sens. Les droits d'accès doivent être distincts selon les fonctions et les rôles (accès aux enregistrements, accès en direct, accès au serveur, autorisation d'extraction, etc.). L'accès au serveur local ainsi qu'au lieu d'hébergement des enregistrements et/ou données extraites est réservé aux personnes autorisées. La consultation des images enregistrées peut être effectuée qu'en cas d'atteinte avérée. Les informations relatives au lieu d'hébergement des données, les mesures techniques (chiffrement, détenteur de la clé) font l'objet d'une analyse spécifique. 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, sans accès à distance. Ainsi aucun réseau sans fils, interconnexion ni Internet n'est utilisé-e.

e. destruction des images : l'article 4 chiffre 3 RU doit déclarer qu'il incombe aux responsables de s'informer régulièrement de la situation. Les données enregistrées doivent être détruites après 72 heures. En cas d'atteintes avérées aux personnes et aux biens, les enregistrements (extraction) peuvent être conservées jusqu'à 100 jours.

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

g. clause de confidentialité : le prestataire mandaté – l'entreprise d'installation du système – ainsi que ses collaboratrices et collaborateurs signent une clause de confidentialité dans la mesure où il s'agit de données sensibles et soumises au secret de fonction.

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

V. Remarques

> **La requérante est rendue attentive au fait que si elle filme ses employés, elle est soumise aux règles de la Loi fédérale du 19 juin 1992 sur la protection des données (RS 235.1 ; LPD). Nous renvoyons la requérante à la prise de position du Préposé fédéral sur le sujet (cf. https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/technologien/videoueberwachung/explications-sur-la-videosurveillance-sur-le-lieu-de-travail.html), de laquelle il ressort notamment que les caméras vidéo doivent être orientées et cadrées de sorte que le personnel de vente ne soit pas constamment filmé et que l'orientation et les réglages de ces dernières doivent donc faire l'objet d'une discussion avec les employés afin que ces derniers connaissent les zones filmées.**

> 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. Les données consultées ne doivent pas être communiquées à des organes publics ou à des personnes privées.

> 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.

Florence Henguely
Préposée cantonale à la protection des données

Annexes
—
- dossier en retour
- formulaire de demande