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 2020-LV-22

PRÉAVIS
du 11 août 2022

À l'attention du Préfet de la Glâne, M. Willy Schorderet

Demande d'autorisation d'installation d'un système de vidéosurveillance avec enregistrement
Sis à la Bibliothèque cantonale et universitaire (ci-après : BCU) de Romont, Route de la Maillarde 6, 1680 Romont

BCU, Rue de la Carrière 22, 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 2 octobre 1991 sur les institutions culturelles de l'État (LICE ; RSF 481.0.1) ;
- le Règlement cantonal du 2 mars 1993 concernant la Bibliothèque cantonale et universitaire (RSF 481.2.11) ;
- 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 BCU (ci-après : la requérante) visant à l'installation d'un système de vidéosurveillance avec enregistrement, sis à BCU-Romont, zone industrielle, Route de la Maillarde 6, 1680 Romont, comprenant 9 caméras _____, sans possibilité de zoom, 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 l'annexe transmis par la Préfecture de la Glâne par courrier du 15 octobre 2020 ainsi que les compléments transmis par la Préfecture de la Glâne par courrier du 1er avril 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). La BCU fait partie des institutions culturelles de l'État (art. 2 al. 1 let. b LICE). Au vu des informations fournies par la requérante, les caméras capturent des images de l'intérieur de la BCU-Romont, en particulier des deux halles de stockage TPR2 et TPR3 et des deux magasins. 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 surveiller les 2 halles de stockage TPR2 et TPR3 et ainsi permettre d'observer les mouvements dans les 2 magasins » (*cf.* art. 1 ch. 5 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 mentionne une volonté de contrôler les mouvements dans les magasins (*cf.* formulaire de demande du 15 octobre 2020).

Aucune information n'est mentionnée concernant d'éventuels vols ou dommages ni d'éventuelles déprédations intervenues dans les lieux ciblés. En outre, aucune plainte pénale n'a été portée à la connaissance de l'ATPrDM.

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. La requérante n'explique pas les risques nécessitant spécifiquement la présence de la vidéosurveillance. L'article 1 chiffre 2 RU mentionne uniquement les risques envisageables (hypothétiques) au vu de la valeur patrimoniale des biens conservés à la BCU-Romont (notamment une intrusion par des personnes non autorisées dans les 2 halles de stockage et leur circulation dans ces halles, en journée comme de nuit).

Une surveillance par un ou plusieurs agents de sécurité est une mesure adéquate. En outre, une limitation de l'accès pour cette zone permettrait un meilleur contrôle du flux dans le magasin et les deux halles

(badge d'entrée, etc.). Un système d'alarme-effraction est en place. La requérante n'apporte, toutefois, aucune information au sujet des bienfaits et des lacunes, voire la portée de ces mesures. Elle n'explique pas en quoi la vidéosurveillance comblerait les limites du système de sécurité mis en place.

1.3 Quant au but

Comme mentionné au point II. 1.1, le but du présent système de vidéosurveillance est « de surveiller les 2 halles de stockage TPR2 et TPR3 et ainsi permettre d'observer les mouvements dans les 2 magasins » (*cf.* art. 1 ch. 5 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, la formulation n'est pas adaptée aux buts énoncés dans le formulaire de demande d'autorisation, l'Autorité conseille vivement la reformulation suivante : « protéger tous les biens de la BCU-Romont et contribuer à la poursuite et répression des infractions réalisées dans les deux halles de stockage TPR2 et TPR3 ainsi dans les deux magasins ». 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, l'article 4 LPrD précise que 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 dans les deux halles de stockage TPR2 et TPR3 ainsi dans les deux magasins est apte à limiter les atteintes 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, toutes les caméras enregistrent les images et comprennent la vision en direct. Aucune information n'a été communiquée selon laquelle les lieux de pose auraient été la cible d'infractions. 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 qui n'est pas doublé d'un suivi en temps réel, mais est 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.

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 (*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) 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 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 A – enregistrement des images et vision en temps réel.** La caméra respecte le principe de la proportionnalité. La vision en temps réel ne respecte pas le principe de la proportionnalité ;

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

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

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

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

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

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

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

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

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

Selon l'article 3 RU, la vision en temps réel est prévue pour des cas exceptionnels. Au vu de la gravité de l'atteinte que soulève un système d'enregistrement doublé d'une vision en temps réel, l'enregistrements est dès lors suffisant ; ce d'autant que la requérante ne soulève pas de risques réels justifiant une telle atteinte. La vision en temps réel n'est pas autorisée. Le paramétrage de l'installation et le RU sont modifiés en ce sens (en particulier l'art. 3)

L'article 4 chiffre 1 RU doit être adapté. Le but est décrit à l'article 1 chiffre 5 RU.

Il ressort du dossier que la visualisation des images fait suite au déclenchement de l'alarme-effraction, voire en cas de soupçon d'un vol constaté (*cf.* art. 3 RU). La consultation des images enregistrées ne peut être effectuée qu'en cas d'atteinte avérée. Le RU est modifié en ce sens.

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 (*cf.* art. 4 ch. 1 RU), sous réserve du chap. II, ch. 1.3.

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

La direction de la BCU est l'organe responsable du système de vidéosurveillance conformément à l'article 2 alinéa 1 lettre a OVid. L'article 2 chiffre 1 RU est modifié en ce sens.

La vision en temps réel n'étant pas admise, la consultation des images enregistrées peut être effectuée qu'en cas d'atteinte avérée (art. 3 RU). L'article 4 RU est d'un chiffre expliquant que toute fonctionnalité permettant d'émettre, d'enregistrer des sons et/ou permettant la reconnaissance faciale n'est pas autorisée.

Aux termes de l'article 5 RU, 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.). Une double authentification est recommandée. À l'article 5 chiffre 1, 1er et 2ème tiret, RU, il est recommandé d'insérer un lien vers l'article 2 chiffre 2 RU. Ces éléments doivent figurer dans le RU.

Concernant la sécurité des données, les informations relatives aux mesures de sécurités mises en place, notamment concernant l'entreprise d'installation (_____) (tels que le chiffrement du transfert et du stockage des données, le détenteur des clés, le contrat y relatif) font défaut. Elles devront faire l'objet d'une analyse spécifique. En outre, 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. Le mandataire ne doit pas pouvoir avoir accès aux données. Le RU doit prévoir que la maintenance ne peut pas être effectuée à distance (*cf.* art. 6 lettre a RU) et doit être effectuée en présence d'un collaborateur de la requérante.

Des précisions font défaut concernant le serveur local (localisation dans le bâtiment nécessaire). Le RU doit préciser que le système de stockage et d'hébergement des données (et/ou le *back-up*) est protégé dans un lieu adéquat en Suisse, fermé à clé et non accessible aux personnes non autorisées. 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 nécessaire. L'hébergement des données est local,

sans accès à distance. Les images enregistrées et celles extraites doivent être stockées sur un support physique indépendant, sans accès à distance possible. Le RU est modifié en ce sens.

Le RU déclare que l'organe responsable s'assure des mesures techniques et organisationnelles concernant l'accès des personnes autorisées aux enregistrements, notamment s'agissant des appareils utilisés.

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

Concernant la durée de conservation, le Préposé fédéral à la protection des données et à la transparence (ci-après : PFPDT) recommande une durée de conservation de 24 à 72 heures[2]. Le Conseil d'État explique dans son Message relatif à la vidéosurveillance qu'« en ce qui concerne le délai de destruction des images enregistrées, […] le projet (let. e) propose un délai qui est suffisant pour que la personne qui visionne les images soit en mesure de réagir (information donnée à son supérieur ; dénonciation pénale, …). Sous cet angle, un délai maximal de 7 jours semble adéquat. […] Un tel délai, jugé admissible par le Tribunal fédéral, est suffisant pour que la collectivité puisse réagir et prendre le cas échéant la décision de dénoncer pénalement les comportements visionnés » (*cf.* BGC novembre 2010 1967, p. 1969). Comme la vidéosurveillance est souhaité pour « surveiller les 2 halles de stockage TPR2 et TPR3 et ainsi permettre d'observer les mouvements dans les 2 magasins » (*cf.* art. 1 ch. 5 RU), la conservation des images devrait être restreinte. Dans cet ordre d'idées, le Tribunal fédéral rappelle qu'il faut distinguer entre les infractions commises contre des biens et celles commises contre des personnes. Les infractions contre les biens étant constatées par les autorités étatiques elle-même (et non sur plainte) une longue durée de conservation n'est pas indispensable en cas d'atteinte (*cf.* ATF 133 I 77, JdT 2007 I 591). Ainsi le délai légal est un maximum qui doit être apprécié à la lumière du cas d'espèce. Les responsables doivent s'informer régulièrement de toute situation pouvant entrer dans le but de la protection. Partant, les données doivent être détruites après 10 jours (automatiquement). En cas d'atteintes avérées aux personnes ou aux biens, les enregistrements peuvent être extraits et conservés jusqu'à 100 jours, de manière sécurisée. Le RU est modifié en ce sens (*cf.* art. 4 ch. 3 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)

Un article relatif au droit d'accès est 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.

---

[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).

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.). Le RU prévoit que la clause de confidentialité est annexée au RU.

10. Déclaration de fichier

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

[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 la **BCU-Romont**, à la Route de la Maillarde 6, 1680 Romont

par

la Bibliothèque cantonale et universitaire, Rue de la Carrière 22, 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, des **caméras A à I.** En effet, il n'est pas autorisé de vision en temps réel ;

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 : l'article 4 chiffre 1 RU est adapté. Le but est décrit à l'article 1 chiffre 5 RU. La consultation des images enregistrées ne peut être effectuée qu'en cas d'atteinte avérée. L'article 3 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 la direction de la BCU.

La vision en temps réel n'étant pas autorisée, le paramétrage de l'installation et le RU sont modifiés en ce sens (en particulier l'art. 3).

L'article 4 RU est complété d'un chiffre expliquant que toute fonctionnalité permettant d'émettre, d'enregistrer des sons et/ou permettant la reconnaissance faciale n'est pas autorisée. Le RU précise que la consultation des images enregistrées ne peut être effectuée qu'en cas d'atteinte avérée.

Les exigences des art. 18 et 12*b* al. 1 let. b LPrD sont respectées. Un contrat particulier doit être conclu. Les autorisations d'accès doivent spécifiquement être distinguées selon l'accès aux enregistrements et les autres types d'autorisation (extraction, serveur local, etc.). 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. Le RU doit préciser que le système de stockage et d'hébergement des données (et/ou le *back-up*) est protégé dans un lieu adéquat en Suisse, fermé à clé et non accessible aux personnes non autorisées. Les images enregistrées et celles extraites doivent être stockées sur un support physique indépendant, sans accès à distance possible. 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.

Le RU déclare que l'organe responsable s'assure des mesures techniques et organisationnelles concernant l'accès des personnes autorisées aux enregistrements, notamment s'agissant des appareils utilisés.

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 automatiquement après 10 jours. 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