ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

La Préposée cantonale à la protection des données

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08, F +41 26 305 59 72
www.fr.ch/atprd

Réf. : FH/nk 2019-LV-13

PRÉAVIS
du 18 mars 2021

À l'attention du Préfet de la Sarine, M. Carl-Alex Ridoré

Demande d'autorisation d'installation de vidéosurveillance avec enregistrement

École de culture générale Fribourg, Avenue du Moléson 17, 1700 Fribourg

I. Généralités

Vu

- les articles 12, 24 et 38 de la Constitution du canton de Fribourg du 16 mai 2004 (Cst ; 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 du 29 juin 1999 sur la sécurité des données personnelles (RSD ; RSF 17.15) ;
- la Loi cantonale du 11 avril 1991 sur l'enseignement secondaire supérieur (LESS ; RSF 412.0.1) ;
- le Règlement du 27 juin 1995 sur l'enseignement secondaire supérieur (RESS ; RSF 412.0.11) ;
- le Règlement du 10 juin 2008 concernant les études en écoles de culture générale (RECG ; 412.4.21),

l'Autorité cantonale de la transparence et de la protection des données (ATPrD) formule le présent préavis concernant la requête de l'École de culture générale Fribourg (ci-après : ECGF) visant à l'installation d'un système de vidéosurveillance avec enregistrement, sis à l'ECGF, Avenue du Moléson 17, 1700 Fribourg, comprenant 9 caméras de type _____, fonctionnant à des horaires différenciés (cf. III, ch. 2) et 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 Sarine par courrier du 26 novembre 2019, les premiers compléments transmis par la Préfecture de la Sarine par courrier du 29 janvier 2020, la vision locale du 25 août 2020 et son procès-verbal ainsi que les compléments transmis par l'ECGF par courrier du 13 octobre 2020 et courriel du 2 février 2021.

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 et de

l'extérieur des trois bâtiments scolaires de l'ECGF (A, B et C), en particulier des entrées et des couloirs. 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. Il est d'abord examiné les risques (cf. II), ensuite 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 et le respect de la confidentialité (cf. III, ch. 1 à 9).

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 « la prévention des actes de vandalisme et l'identification des personnes ayant causé des dégâts ou commis des infractions dans le périmètre de l'ECGF » (cf. art. 1 ch. 3 du Règlement d'utilisation ; ci-après : RU).

Une analyse des risques, à la lumière du principe de la proportionnalité, figure au dossier. Sur la base de la vision locale du 25 août 2020 et 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 les automates à boissons et snacks (entrée du bâtiment A et cafétéria du bâtiment C) sont fréquemment « bousculés » pour faire tomber de la monnaie. Ils ont, en outre, été forcés quatre fois en cinq ans. Le personnel (bâtiment A) a pris l'habitude de travailler avec les portes ouvertes pour pouvoir entendre tout bruit suspect. Le secrétariat et le bureau de la direction ont été visités trois fois sur dix ans (bâtiment A). Un coffre-fort a été acheté pour stocker les éléments les plus importants en terme de confidentialité, mais l'espace s'avère peu satisfaisant.

Concernant le bâtiment C, _____ estime une perte annuelle de CHF 1'500 par le vol de boissons en self-service. Toutes les deux semaines, des vols ont lieu dans les vestiaires de la salle de sport. À noter qu'il y a trois ans, un vol pour un montant de CHF 14'000 a été enregistré. Il s'agit d'un vol réalisé par l'obtention illicite d'une clé. Par courriel du 2 février 2021, il a été porté à la connaissance de l'Autorité que des vols ont eu lieu dans les vestiaires des salles de sport les 8, 21 et 22 ainsi que la semaine du 25 au 29 janvier 2021. Il s'agit d'un ou plusieurs téléphones portables, d'argent liquide ainsi que divers objets personnels. Il n'a pas été précisé si les vols ont eu lieu dans le vestiaire des professeurs fermé à clé ou dans les vestiaires des élèves non fermés à clé. 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. La surveillance de la part du personnel, l'achat d'un coffre-fort, la fermeture des vestiaires à clé pendant les périodes de cours et le regroupement des objets de valeurs dans le vestiaire des professeurs de sport fermé à clé sont jugés insatisfaisant par l'ECGF. Il sied de

noter que l'usage de casiers individuels de qualité a été éprouvé dans bons nombres d'écoles du Canton et jugés satisfaisant pour mettre fins aux vols d'objets personnels d'élèves. L'ECGF reconnaît que les casiers présents sur le site ne sont pas de bonne qualité et installés trop loin des secteurs en question. À noter que les objets personnels de valeur devraient, à tout le moins, être gardés sous clé lors des cours de sport. Des écoles du Canton ont mis en place des systèmes de paiement sur facture ou de recharge de carte d'étudiant-e-s pour leur éviter de transporter de trop grandes sommes d'argent. Ces mesures restent encore à être éprouvées sur le site de la requérante.

Concernant les derniers vols annoncés (cf. courriel du 2 février 2021), il sied de relever que des précisions font défaut, notamment concernant le lieu des vols, puisque selon les informations précitées, tous les objets de valeur sont mis sous clés dans le vestiaire des professeurs.

1.3 Quant au but

Comme mentionné au point II. 1.1, le but du présent système de vidéosurveillance est « la prévention des actes de vandalisme et l'identification des personnes ayant causé des dégâts ou commis des infractions dans le périmètre de l'ECGF » (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)).

Il paraît envisageable que le moyen projeté permette de remplir les but poursuivis et de limiter les risques précités.

III. Conditions

1. Exigence de la base légale

L'article 38 Cst prévoit 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 ». En l'occurrence, c'est le cas dans la LVid. En outre, conformément à l'article 4 LPrD, le traitement de données personnelles ne peut se faire que si une disposition légale le prévoit, ce qui est le cas également.

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), le droit au respect de la sphère privée (art. 12 al. 1 Cst et 8 CEDH), le droit d'être protégé contre l'emploi abusif des données personnelles (art. 12 al. 2 Cst) et la liberté de réunion (art. 24 Cst ; cf. FLÜCKIGER/AUER, La vidéosurveillance dans l'œil de la Constitution fédérale, AJP/PJA 2006, p. 931).

Si la mesure paraît apte à atteindre le but visé, il n'en demeure pas moins que la surveillance doit être adéquate, c'est-à-dire apte à atteindre le but visé mais également 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 publics (cf. Arrêt TC FR 601 2014 46 du 20 août 2015, consid. 2b/cc). En l'état, on peut dès lors admettre que l'installation des caméras à l'extérieur des bâtiments de l'ECGF 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, p. 3). 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. Ces images ne sont pas visionnées en temps réel mais uniquement consultées lors d'une atteinte avérée.

Sous l'angle de la nécessité, plusieurs mesures moins intrusives sont envisageables, telles que la mise en place de casiers adéquats et solides pour les biens personnels des élèves et les objets de valeur aux lieux stratégiques et utiles ainsi que la mise en place de système de paiement alternatif (facture, carte étudiant rechargeable, etc.). Il sied de relever que certaines écoles du Canton ont vu disparaître les vols une fois ces mesures mises en place. En l'espèce, la requérante souffre principalement de vols fréquents. Aucune déprédation de bâtiment n'est reportée.

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 (cf. TC FR 601 2014 46, consid. 2b/cc et réf. citées). **S'agissant des automates à boissons et à snacks ainsi qu'aux frigos à boissons**, ceux-ci ne répondent pas à un intérêt public, ni ne s'inscrivent dans la mission publique de l'établissement scolaire. Il importe de rappeler que l'école bénéficie d'une cafétéria avec du personnel. Notons en outre qu'il n'est pas possible pour un-e étudiant-e du Canton qui souhaite suivre la même formation de pouvoir s'inscrire dans un autre établissement du district. En effet, les ECGF du Canton sont au nombre de deux : celle de Fribourg et celle du Collège du Sud, à Bulle (art. 3 al. 2 et art. 15 al. 3 LESS, art. 15 al. 1 RESS et art. 1 al. 1 RECG). Il y a dès lors une obligation de s'inscrire à l'ECGF pour ce cursus scolaire. Cela étant, la surveillance envisagée est bien trop intrusive au vu des intérêts défendus pour les automates et frigos à aliments et au vu des mesures moins intrusives possibles.

Concernant le secrétariat et le bureau de la direction, l'objectif de ces lieux s'inscrit dans la mission de l'établissement de veiller au bon déroulement de la formation et des examens (art. 19 al. 4 RECG). Il y a ainsi un intérêt public. Ce nonobstant, l'horaire envisagé est de 00h00 à 24h00. Il est difficile de soutenir une telle argumentation (pas de nécessité). Premièrement, la présence du personnel en journée et pendant les horaires scolaires rend difficile l'accès non-autorisé aux locaux. Il se justifie de ne filmer que les lieux indispensables à la surveillance et dans un horaire proportionné (aptitude, nécessité et proportionnalité au sens étroit). Deuxièmement, 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). Par conséquent, l'installation du système de vidéosurveillance

envisagé étant très intrusive, une grande retenue doit être opérée selon les lieux de pose des caméras envisagées.

Afin d'avoir une vue générale, l'analyse sous l'angle de la proportionnalité est faite pour chaque caméra, de manière chronologique :

- **Camera 1 – entrée bâtiment A, niveau 0 – enregistrement des images 24h/24. Il n'y a pas de vision en temps réel.** La caméra vise la surveillance des automates à boissons et snacks à l'entrée du bâtiment A. La caméra ne respecte pas le principe de la proportionnalité (cf. III, ch. 2).

- **Camera 2 – administration bâtiment A, niveau 0 – enregistrement des images 24h/24. Il n'y a pas de vision en temps réel.** Lorsque des collaborateurs et collaboratrices risquent d'être fréquemment filmé-e-s, il sied de rappeler que lien de subordination limite fortement le consentement de ceux-ci à une telle vidéosurveillance. Le Préposé fédéral à la protection des données (PFPDT) précise que l'employé-e « ne doit pas être filmé par la caméra, si ce n'est exceptionnellement, car cela peut constituer une atteinte à sa santé. L'installation de caméras de surveillance peut être envisagée à l'extérieur des bâtiments et sur les parkings, dans les voies d'accès et halls d'entrée, dans les couloirs ou corridors » (cf. https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/technologien/videoueberwachung/explications-sur-la-videosurveillance-sur-le-lieu-de-travail.html). Au vu de l'intérêt public protégé, l'examen de la proportionnalité est soutenu hors des horaires scolaires soit de 18h00 à 07h00 (comme expliqué ci-haut ; cf. III, ch. 2).

- **Camera 3 – sélecta et micro-onde bâtiment C, niveau -1 – enregistrement des images de 07h00 à 20h00. Il n'y a pas de vision en temps réel**. La caméra ne respecte pas le principe de la proportionnalité (cf. III, ch. 2).

- **Camera 4 – frigo bâtiment C, niveau -1 – enregistrement des images de 07h00 à 20h00. Il n'y a pas de vision en temps réel.** La caméra ne respecte pas le principe de la proportionnalité (cf. III, ch. 2).

- **Camera 5 – couloir sport bâtiment C, niveau -2 – enregistrement des images de 06h00 à 24h00. Il n'y a pas de vision en temps réel.** Pendant les horaires scolaires, les étudiant-e-s subissent des vols d'objets personnels laissés dans les vestiaires. Il appartient à l'ECGF de mettre en place des casiers solides à proximité, voire de veiller à ce qu'aucun objet personnel de valeur ou argent liquide ne restent dans les vestiaires (mise sous clé dans les locaux des professeurs de sport par exemple). La vidéosurveillance est ici disproportionnée au vu du dispositif pouvant être mis en place (cf. II, ch. 1.2 ; III, ch. 2). La caméra ne respecte pas le principe de la proportionnalité.

- **Camera 6 – couloir sport bâtiment C, niveau -2 – enregistrement des images de 06h00 à 24h00. Il n'y a pas de vision en temps réel.** La caméra ne respecte pas le principe de la proportionnalité (cf. il est renvoyé à l'argumentation de la caméra 5).

- **Camera 7 – couloir sport bâtiment C, niveau -2 – enregistrement des images de 06h00 à 24h00. Il n'y a pas de vision en temps réel.** La caméra ne respecte pas le principe de la proportionnalité (cf. il est renvoyé à l'argumentation de la caméra 5).

- **Camera 8 – couloir sport bâtiment C, niveau -2 – enregistrement des images de 06h00 à 24h00. Il n'y a pas de vision en temps réel.** La caméra ne respecte pas le principe de la proportionnalité (cf. il est renvoyé à l'argumentation de la caméra 5).

- **Camera 9 – entrée extérieur bâtiment C, niveau -2 – enregistrement des images de 06h00 à 24h00. Il n'y a pas de vision en temps réel.** Au vu du lieu de situation de la caméra, l'examen de la proportionnalité est soutenu hors des horaires scolaires soit de 18h00 à 07h00 (comme expliqué ci-haut ; cf. III, ch. 2).

La prise en compte de l'intérêt public de l'établissement fait que deux caméras ont été admises hors horaires scolaires (cf. caméras 2 et 9) ; ce d'autant qu'il peut s'agir de mineurs. L'horaire hors scolaire doit être précisé dans le RU. Au surplus, toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons ne doit pas être utilisée. 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)

Aux termes de la législation, le système doit être signalé à ses abords de manière adéquate (art. 4 al. 1 let. b LVid). Le RU mentionne uniquement que « la direction de l'ECGF publie sur son site lnternet la liste des lieux placés sous vidéosurveillance. Dans la mesure du possible, elle complète ces informations de plans de situation » (cf. art. 1 ch. 6 RU). 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).

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

De manière générale, le respect de la législation demande un RU précis en matière de mesures de sécurités. Partant, les chiffres modifiés et/ou ajoutés de l'article 5 RU peuvent prendre la tournure suivante :

1. *Les données informatiques sont protégées par l'organe responsable du fichier de la façon suivante :*
    - *une autorisation personnelle d'accès est délivrée aux personnes autorisées (cf. art. 2 ch. 2) ;*
    - *les personnes autorisées bénéficient d'un accès (mot de passe) et modifient régulièrement leur mot de passe ;*
    - *les titulaires d'autorisation personnelle consultent les images enregistrées qu'en cas de nécessité, à savoir en cas d'atteinte avérée ;*
    - *une double authentification est recommandée.*
2. *Toute activité effectuée sur le système ou sur une des applications informatiques sera automatiquement enregistrée et répertoriée à des fins de contrôle et/ou de reconstitution.*
3. *Le système de stockage et d'hébergement des données (et/ou la back-up) doivent être protégés dans un lieu adéquat en Suisse, fermé à clé et non-accessible aux personnes non-autorisées.*

4. *Les images enregistrées et celles extraites doivent être stockées sur un support physique indépendant, sans accès à distance possible (réseaux sans fils ou internet) et, est remis, le cas échéant, au procureur ou au juge en charge de la procédure. Seules les personnes autorisées ont accès au serveur local, qui se trouve sur le site de l'ECGF.*
5. *L'organe responsable s'assure des mesures techniques et organisationnelles concernant l'accès des personnes autorisées aux enregistrements et aux extractions, notamment s'agissant des appareils utilisés.*

Concernant la sécurité des données (hébergement, chiffrement, accès, etc.), il ressort des informations transmises qu'un serveur local se situe dans une armoire fermée à clé dans le bureau de l'Administrateur de l'ECGF. L'article 5 chiffre 4 RU dispose que les enregistrements sont stockés sur un support physique indépendant, sans accès à distance (réseaux sans fils ou Internet), de sorte que les enregistrements devraient uniquement être hébergés *in situ* de manière sécurisée et que seules les personnes autorisées ont accès au serveur local. La question de la sous-traitance se pose, à savoir si l'ECGF a sous-traité le traitement à une entreprise ou un fournisseur. Des précisions et des garanties à ce sujet sont nécessaires, telles qu'un contrat, une clause de confidentialité et les informations relatives à la maintenance du système.

En cas d'atteinte avérée, l'image doit pouvoir être extraite pour permettre l'ouverture d'une procédure, voire en attente de la demande du juge. En conformité avec la loi, il importe d'enregistrer (« extraire ») l'image sur un support séparé afin que les images non-nécessaires puissent être supprimées dans le délai de 7 jours (cf. III, ch. 6). L'article 4 RU est complété d'un chiffre distinguant les enregistrements continus standards des enregistrements faisant suite à une extraction de données ; d'un chiffre expliquant que les images sont uniquement enregistrées ; et d'un chiffre expliquant que toute fonctionnalité permettant d'émettre et/ou enregistrer des sons n'est pas autorisée.

« Les chiffres modifiés et/ou ajoutés de l'article 4 RU peuvent prendre la tournure suivante :

1. *Les données enregistrées ne devront être utilisées que dans le cadre du but défini à l'article 1 alinéa 3 ci-dessus.*
2. *Les images enregistrées ne sont pas visionnées en temps réel.*
3. *Les titulaires d'autorisation personnelle (cf. art. 2 ch. 2) consultent les images enregistrées qu'en cas de nécessité, à savoir en cas d'atteinte avérée.*
4. *Les personnes autorisées à consulter les données sont susceptibles d'être interrogées en tout temps, y compris au-delà de l'exercice de leurs fonctions, sur les données qu'elles auront visionnées ou sur leurs agissements en relation avec ces données.*
5. *Les données enregistrées sont automatiquement détruites après 7 jours. En cas d'atteinte avérée aux personnes ou aux biens, les données enregistrées sont extraites sur un support informatique sécurisé et sont détruites après 100 jours au maximum.*

   Un protocole de destruction est conservé.
6. *Des copies ou impressions peuvent être effectuées mais doivent être détruites dans les mêmes délais que les originaux. Un protocole de copie est conservé.*
7. *La commercialisation d'éventuelles impression et reproduction est interdite*
8. *Toute communication de données est interdite, en dehors du cadre légal (art. 4 al. 1 let. e LVid).*
9. *Toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons n'est pas autorisée. »*

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

La durée de conservation proposée est trop longue. 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[1]. 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 » (BGC novembre 2010 1967, p. 1969). Ainsi, le délai légal est un maximum qui doit être apprécié à la lumière du cas d'espèce. Par ailleurs, les responsables doivent s'informer régulièrement de toute situation pouvant entrer dans le but de protection. Partant, les données enregistrées doivent être détruites après 7 jours. En cas d'atteintes avérées aux personnes ou aux biens, les enregistrements peuvent être conservées jusqu'à 100 jours (cf. art. 4 ch. 3 RU). L'article 4 chiffre 3 RU est modifié dans ce sens.

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

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

IV. Conclusion

Dans le cadre de la demande d'installation du système de vidéosurveillance avec enregistrement sis à l'Avenue du Moléson 17, 1700 Fribourg

par

l'École de Culture Général Fribourg,

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

- préavis **défavorable** à la demande d'installation des caméras **n° 1, n° 3 à n° 8** avec enregistrement ;
- préavis **favorable** à la demande d'installation des caméras **n° 2 et n° 9** 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 : afin de limiter l'atteinte aux droits de la personnalité à ce qui est strictement nécessaire, l'utilisation des caméras sera limitée à ce qui est nécessaire : à savoir en dehors des horaires scolaires soit de 18h00 à 7h00 la semaine ; toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons ne doit pas être utilisée.

c. signalement : l'article 1 chiffre 6 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 ».

d. sécurité des données : les articles 4 et 5 RU doivent être préciser (cf. ci-dessus). Des précisions et des garanties au sujet de l'éventuelle sous-traitance sont nécessaires, telles qu'un contrat, une clause de confidentialité et les informations relatives à la maintenance du système.

e. destruction des images : l'article 4 chiffre 3 RU doit déclarer qu'il incombe aux responsables de s'informer régulièrement de la situation à l'ECGF. Ainsi, les données enregistrées doivent être détruites après 7 jours. En cas d'atteintes avérées aux personnes et aux biens, les enregistrements 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.

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 sera publié.

Florence Henguely
Préposée cantonale à la protection des données

Annexes
—
- dossiers complément du 29 janvier 2020 et du 13 octobre 2020 en retour
- formulaire de demande