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-1

PRÉAVIS
du 28 janvier 2021

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

Demande d'autorisation d'installation de vidéosurveillance avec enregistrement sis au **Foyer Sainte-Elisabeth**, Route du Botzet 4-6, 1700 Fribourg

p. a. ORS Service AG, Route du Petit-Moncor 1A, 1752 Villars-sur-Glâne

I. Généralités

Vu

- les art. 12, 24 et 38 de la Constitution du canton de Fribourg du 16 mai 2004 (Cst ; RSF 10.1) ;
- l'art. 5 al. 2 de la Loi cantonale du 7 décembre 2010 sur la vidéosurveillance (LVid ; RSF 17.3) ;
- l'art. 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),

l'Autorité cantonale de la transparence et de la protection des données (ATPrD) formule le présent préavis concernant la requête de la société ORS Service AG (ci-après : ORS) visant à l'installation d'un système de vidéosurveillance avec enregistrement dans les locaux du Foyer Sainte-Elisabeth, Route du Botzet 4-6, 1700 Fribourg, comprenant 6 caméras – dont 1 de type _____, 1 de type _____, 2 de type _____, et 2 de type _____, fixes, 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, de son Règlement d'utilisation et des annexes, transmis par la Préfecture de la Sarine par courrier du 7 janvier 2019, de la vision locale du 8 septembre 2020 et son procès-verbal ainsi que des compléments transmis par l'ORS par courriel du 13 octobre 2020. Le système de vidéosurveillance fait l'objet de ce préavis pour autant que le champ de vision de ses caméras couvre tout ou partie de lieux publics (art. 2 al. 1 LVid). Sont des lieux publics, les immeubles et lieux qui n'appartiennent pas au domaine public mais qui sont affectés à l'administration publique (cf. art. 2 al. 2 let. b LVid). Depuis le 1er janvier 2008, ORS est mandatée par le canton de Fribourg pour l'hébergement et l'encadrement des requérants d'asile attribués au Canton. Au vu des informations fournies par le requérant, les caméras capturent des images des entrées, de la réception, de la salle à manger et du salon du Foyer Ste-Elisabeth. 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. chap. 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. chap. 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 « de prévenir des atteintes aux résidents du foyer et au personnel d'encadrement et permettra d'observer les entrées du foyer (no 4 et 6) ainsi que différentes surfaces internes (voir plans et photos annexés). Il s'agira également de prévenir des dégâts aux biens. En cas d'infractions il contribuera à l'identification des personnes impliquées » (cf. art. 1 ch. 3 du Règlement d'utilisation ; ci-après : RU).

Dès lors, il appert que le système prévoit de poursuivre trois buts :

1) prévenir les atteintes aux personnes et aux biens ;
2) observer les entrées et les locaux du site ;
3) contribuer à l'identification des personnes impliquées en cas d'infraction.

Une analyse des risques, à la lumière du principe de la proportionnalité, figure au dossier. Sur la base de la vision locale du 8 septembre 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. L'analyse des risques relate quatre grands types de risques : rixes et bagarres, entrées clandestines non-autorisées, comportements répréhensibles (harcèlement, trafic de substances illicites, etc.) et atteintes aux mineurs (protection contre des scènes choquantes). Quoique l'analyse fasse état de risques potentiellement importants, le dossier ne fait pas fait mention de dépôt de plainte ni de déprédation. En outre, il est bien concevable que de telles atteintes peuvent survenir à l'encontre tant des résident-e-s que du personnel encadrant, que du mobilier, des fournitures et des locaux mis à disposition. À noter qu'il est question d'un centre de vie de personnes en situation d'asile. En effet, l'ORS est mandatée par le canton de Fribourg pour l'hébergement et l'encadrement des requérants d'asile attribués au Canton. Par ailleurs, il a été rappelé lors de la vision locale du 8 septembre 2020 que le Foyer Ste-Elisabeth est aujourd'hui considéré en zone verte depuis quelques années déjà.

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. En l'espèce, il ressort du dossier que le Foyer Ste-Elisabeth est pourvu d'un veilleur en soirée et les week-ends. Le Foyer bénéficie ainsi d'une présence continue.

L'ORS a opté pour des caméras aux entrées et lieux d'interaction et a jugé inutile de placer la vidéosurveillance à l'arrière du foyer où un éclairage a été privilégié. Aucune autre méthode n'a été mise en place, ni éprouvée.

1.3 Quant au but

Comme mentionné au point II. 1, le but du présent système est « de prévenir des atteintes aux résidents du foyer et au personnel d'encadrement et permettra d'observer les entrées du foyer (no 4 et 6) ainsi que différentes surfaces internes (voir plans et photos annexés). Il s'agira également de prévenir des dégâts aux biens. En cas d'infractions il contribuera à l'identification des personnes impliquées ». Dès lors, le système (cf. RU) prévoit de poursuivre trois buts : prévenir les atteintes aux personnes et aux biens, observer les entrées et les locaux du site et contribuer à l'identification des personnes impliquées en cas d'infraction.

Cela étant, il ressort du dossier que la volonté soit en outre de surveiller les allées et venues (éventuelle entrée clandestine), de prévenir et stopper de potentiels trafics de substances illicites, d'identifier les personnes présentes notamment en cas d'incendie, de préserver les mineurs de scènes choquantes voire traumatisantes, d'éviter que les objets pointus ou contondants soient utilisés à des fins nocives et d'éviter des vols (cf. Analyse des risques pour la pose d'un système de vidéosurveillance au Foyer Ste-Elisabeth, route du Botzet 4 à Fribourg).

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).

Deux des buts figurant à l'article 1 chiffre 3 RU entrent dans le champ d'application de la LVid : la prévention des atteintes aux personnes et aux biens et la contribution à l'identification des personnes impliquées en cas d'infraction. Dès lors, il paraît envisageable que le moyen projeté permette de remplir les buts poursuivis.

Or l'observation des allées et venues, la lutte contre les trafics illicites, l'identification des personnes présentes en cas d'incendie notamment le contrôle d'identités des personnes présentes, le fait de préserver les mineurs de scènes choquantes voire traumatisantes ne sont pas conformes à la législation. Il est rappelé que la vidéosurveillance n'est pas un instrument pour faire respecter des instructions ou le règlement du foyer. Le Tribunal cantonal rappelle que le but tendant à « utilisation conforme aux instructions du matériel » est manifestement contraire à la LVid et ne peut être admis (cf. Arrêt TC FR 601 2014 46 du 20 août 2015, consid. 3a). Il est de la responsabilité des collaborateurs et collaboratrices d'informer suffisamment les résidents des règles et attentes (notamment en termes de mesures de protection d'incendie, d'identification, etc.). Partant, ces buts ne sauraient être observés au moyen de la vidéosurveillance sans que l'on puisse constater une disproportion excessive entre le but poursuivi et le système de vidéosurveillance projeté. Sans oublier que des moyens bien moins restrictifs que la vidéosurveillance peuvent être mis en place pour atteindre ces buts.

L'article 1 chiffre 3 RU doit, dès lors, être modifié pour ne comprendre que les buts conformes à la LVid : soit la prévention des atteintes aux biens et/ou aux personnes et la contribution à la poursuite et à la répression des infractions.

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 nécessité est mesurée par l'absence d'autres mesures moins incisives théoriquement envisageable. Il est indéniable que des alternatives efficaces à la vidéosurveillance existent, sans pour autant remettre en question la nécessité de celle-ci (cf. TC FR 601 2014 46, consid. 2b/cc). La mesure restrictive doit être apte à produire les résultats escomptés (aptitude) et ceux-ci ne doivent pas pouvoir être atteints par une mesure moins incisive (nécessité). Toute restriction allant au-delà du but visé est proscrite. La proportionnalité au sens étroit requiert que l'intérêt public à la prévention et à la répression d'infractions (dégâts matériels, atteintes à la personne) l'emporte sur l'intérêt privé au respect des libertés personnelles des personnes (cf. Arrêt TC FR 601 2014 46, consid. 2b/cc et réf. citées). 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 de vidéosurveillance au Foyer Ste-Elisabeth est apte à prévenir les atteintes aux personnes et/ou aux biens, à contribuer à la poursuite et à la répression des infractions et peut comporter un effet dissuasif. Il sied, toutefois, de noter que certains buts ne passent pas l'examen de la proportionnalité.

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, l'enregistrement et la vision en direct sont prévus. Il s'agit ainsi d'une atteinte grave à la personnalité. Les intérêts publics protégés doivent ainsi être conséquents. Pour l'heure, le dossier ne fait état d'aucune

plainte, ni aucun dommage chiffré. Selon l'article 17 de l'Ordonnance 1 sur l'asile relative à la procédure (OA 1), entrée en vigueur le 1er janvier 2020, « aucun dispositif de vidéosurveillance ne doit être installé aux endroits dans lesquels la sphère privée et intime des personnes se trouvant dans les bâtiments gérés par le SEM doit être respectée » (Rapport explicatif du 4 avril 2019 sur la modification des ordonnances d'exécution des normes procédurales et systèmes d'information, p. 11). En l'espèce, il est question d'un centre régit sous mandat cantonal. Il sied ainsi de s'inspirer du principe tiré de la législation précitée, bien qu'elle ne concerne pas directement le cas d'application. 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). 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 :

- **Caméras 1 à 4** : le but des caméras aux entrées est l'identification des résident-e-s, des visiteurs ainsi que la possibilité de retrouver l'itinéraire de personnes disparues.

  Lorsqu'un enregistrement est doublé d'une vision directe, l'atteinte est considérée comme particulièrement grave (FLÜCKIGER/AUER, op. cit., p. 934). La volonté de la requérante étant de limiter les accès clandestins à ses bâtiments, le contrôle aux entrées de l'identité des visiteurs se comprend. Ce nonobstant, il ne s'agit pas d'un centre grand en taille. La présence continue du personnel offre une surveillance presque ininterrompue. Par ailleurs, l'identification des visiteurs n'est pas conforme au but de la LVid ; dès lors qu'autant l'intérieur que l'extérieur du site est soumis à la LVid. Pour le cas de disparition(s), il n'a pas été suffisamment étayé la fréquence des disparitions de personnes pour appuyer un impératif besoin d'une vision en continue. En effet, la recherche de personnes disparues nécessite essentiellement un accès aux images enregistrées. Ce qui est admis en l'espèce.

  Camera 1 – entrée bâtiment 3 – enregistrement des images et vision en temps réel.

  Seul l'enregistrement est octroyé. Le personnel, les résident-e-s et les visiteurs doivent être informé-e-s de l'enregistrement ;

  Camera 2 – entrée Botzet 4 – enregistrement des images et vision en temps réel.

  S'agissant de l'entrée du personnel – se référant à la jurisprudence du Tribunal cantonal de Fribourg – « directement centrée sur le parking réservé aux employés, la caméra limite considérablement les libertés de ces derniers dans leurs allées et venues, en ce sens que l'on peut ainsi notamment savoir quand ils arrivent et partent, avec qui ils échangent des propos ou partagent un véhicule, éléments manifestement sans aucun lien avec le but visé par la vidéosurveillance. Il s'agit par conséquent d'examiner si d'autres mesures permettent d'atteindre le but visé sans porter atteinte aux intérêts notamment des employés qui sont directement filmés à leur arrivée et leur départ, restreignant au maximum les zones surveillées. Rappelons que les personnes non-concernées doivent en effet avoir la possibilité d'éviter le

champ de la caméra et qu'il n'existe pas de « passage obligé » ni de surveillance vidéo dite « totale » » (cf. Arrêt TC FR 601 2016 127 du 18 mai 2017 consid. 3c). Il sied de mettre un cache ou « bloc noir » pour enlever les véhicules du champ de vision. En outre, les images ne peuvent être utilisées à des fins de contrôle du personnel.

Partant, seul l'enregistrement est octroyé. Le personnel, les résident-e-s et les visiteurs doivent être informé-e-s de l'enregistrement ;

Camera 3 – entrée Botzet 6 – enregistrement des images et vision en temps réel.

Seul l'enregistrement est octroyé. Le personnel, les résident-e-s et les visiteurs doivent être informé-e-s de l'enregistrement ;

Camera 4 – réception – enregistrement des images et vision en temps réel.

Seul l'enregistrement est octroyé. Le personnel, les résident-e-s et les visiteurs doivent être informé-e-s de l'enregistrement ;

- **Camera 5 – salon – enregistrement des images et vision en temps réel.** Comme expliqué, « aucun dispositif de vidéosurveillance ne doit être installé aux endroits dans lesquels la sphère privée et intime des personnes se trouvant dans les bâtiments gérés par le SEM doit être respectée » (Rapport explicatif du 4 avril 2019 sur la modification des ordonnances d'exécution des normes procédurales et systèmes d'information, p. 11). L'article 17 OA 1 précise à son alinéa 2 qu'il est interdit d'utiliser la vidéosurveillance dans les chambres, les douches et les toilettes des centres d'hébergement. Quoique le salon ne figure pas sur la liste précitée, il importe de mentionner qu'il se trouve être le seul lieu de détente où les résident-e-s peuvent profiter du Wifi. L'installation d'un système de vidéosurveillance y serait très intrusive. Bien qu'il est reconnu une certaine utilité à filmer le salon, le principe de proportionnalité ne peut admettre la vision en temps réel tout au long de la journée en sus de l'enregistrement. En effet, la proportionnalité au sens étroit requiert que l'intérêt public à la prévention et à la répression d'infractions (dégâts matériels, atteintes à la personne) l'emporte sur l'intérêt privé au respect des libertés personnelles des personnes (cf. Arrêt TC FR 601 2014 46, consid. 2b/cc et réf. citées). L'analyse des risques présente au dossier n'est pas suffisamment étoffée pour donner un tel poids à l'intérêt public. De nos informations, seule une grosse dispute a été assez fâcheuse dans cet espace. Par ailleurs, il y a du personnel présent sur place. Partant, seul l'enregistrement est octroyé pour ce lieu ;

- **Camera 6 – salle à manger – enregistrement des images et vision en temps réel.** Comme expliqué, « aucun dispositif de vidéosurveillance ne doit être installé aux endroits dans lesquels la sphère privée et intime des personnes se trouvant dans les bâtiments gérés par le SEM doit être respectée » (Rapport explicatif du 4 avril 2019 sur la modification des ordonnances d'exécution des normes procédurales et systèmes d'information, p. 11). L'article 17 OA 1 précise à son alinéa 2 qu'il est interdit d'utiliser la vidéosurveillance dans les chambres, les douches et les toilettes des centres d'hébergement. Quoique la salle à manger ne figure pas sur la liste précitée, il importe de mentionner que les choix alimentaires sont des préférences qui font parties de la sphère privée. L'installation d'un système de vidéosurveillance y serait très intrusive, il peut être reconnu une certaine utilité à filmer la salle à manger, mais le principe de proportionnalité ne peut admettre la vision en temps réel tout au long de la journée en sus de l'enregistrement. En effet, la proportionnalité au sens étroit requiert que l'intérêt public à la prévention et à la répression d'infractions (dégâts matériels, atteintes à la personne) l'emporte

sur l'intérêt privé au respect des libertés personnelles des personnes (cf. Arrêt TC FR 601 2014 46, consid. 2b/cc et réf. citées). L'analyse des risques présente au dossier n'est pas suffisamment étoffée pour donner un tel poids à l'intérêt public. De nos informations, seule la présence d'objet dangereux fonde cette volonté ainsi qu'un ou deux évènements fâcheux il y a quelque temps déjà. Il sied de relever que d'autres mesures moins intrusives doivent être privilégiées (usage de services et vaisselles dans des matériaux autres : plastique, bio dégradable, etc.). À noter que depuis la crise de la COVID-19, les repas n'ont plus lieux en salle à manger à une heure précise pour l'ensemble des résident-e-s. Avant, il était interdit de manger dans les chambres pour des raisons sanitaires. Désormais, les personnes reçoivent un plateau repas. Par ailleurs, il y a du personnel présent sur place. Partant, seul l'enregistrement est octroyé pour ce lieu.

La vision en temps réel étant refusé, l'écran de la réception est enlevé. Le bureau des responsables comprend un écran et une console de commande (permettant notamment de (re)voir les images enregistrées). La vision en direct est également supprimée des fonctionnalités présentes dans le bureau du responsable. Le RU est modifié, voire précisé, à cet effet.

La prise en compte des besoins particuliers du centre font qu'il est admis un fonctionnement du système de vidéosurveillance 24h/24, 7j/7 en ce qui concerne l'enregistrement ; dès lors que la vision en direct n'est pas admise. À noter qu'au vu du site et de l'analyse des risques présente au dossier, une vision en direct doublée d'un enregistrement 24h/24, 7j/7 ne soutient pas l'examen de la proportionnalité. Toutefois, 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)

Des documents à disposition, il ressort que le signalement est prévu (cf. art. 1 ch. 5 RU).

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).

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

La vision en temps réel n'étant pas admise, il sied d'opérer plusieurs modifications dans le RU.

Concernant la localisation des serveurs et l'hébergement des données, des précisions sont nécessaires à la lumière des conditions générales fournies par courriel du 13 octobre 2020 (CG). De nos informations, les back-up sont sur les serveurs centraux _____. La requérante a un serveur propre dédiée à la vidéosurveillance sur son site (transmission par câble). Le serveur local est dans une armoire fermée à clé dans le bâtiment. 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. Or, il ressort des CG que _____ effectue la maintenance à distance. Au vu des données sensibles, il est vivement conseillé que le mandataire n'ait pas accès aux données et enregistrements et que les données soient uniquement stockées et hébergées au sein du Foyer de manière sécurisée et chiffrée. Le cas échéant, une clause de confidentialité doit être signée (cf. chap. III, ch. 9) avec les collaborateurs concernés de _____.

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 (cf. art. 4 ch. 4, 2ème phr.) ;*

   - *une double authentification est mise en place.*

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 (cf. art. 4 ch. 4). Seules les personnes autorisées ont accès au serveur local, qui se trouve sur le site du Foyer (cf. art. 2 ch. 2).*

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.*

Il sied de noter qu'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 le reste des images puisse être supprimé dans le délai de 7 jours (cf. chap. 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 sont utilisées que dans le cadre du but défini à l'article 1 alinéa 3.*

2. *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.*

3. *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.*

4. *Toutes les données enregistrées sont automatiquement détruites après 7 jours. En cas d'atteinte 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. Ce protocole comprend notamment l'identification de l'enregistrement (date, heure, descriptif d'évènement) ainsi que la date de destruction et la personne autorisée ayant détruit l'enregistrement.

5. *Des copies ou impressions peuvent être effectuées mais doivent être détruites dans les mêmes délais que les originaux. Un protocole de copie est conservé.*

6. *Les images sont uniquement enregistrées.*

7. *Toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons n'est pas autorisée.*

8. *La commercialisation d'éventuelles impression et reproduction est interdite.*

9. *Toute communication de données est interdite, en dehors du cadre légal (art. 4 al. 1 let. e LVid).* »

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

La durée de conservation figurant dans le RU est trop longue. Au vu de l'analyse des risques, notamment pour des cas de disparition, une réaction rapide est attendue. 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, des informations en notre possession, il ressort qu'un veilleur assure la présence en soirée et les week-end, de sorte que les atteintes sont connues à très brève échéance (veilleur ou collaborateurs et collaboratrices présent-e-s de jour).

Partant, les données enregistrées sont détruites après 7 jours. L'article 4 RU doit être modifié en ce sens. En cas d'atteintes avérées aux personnes ou aux biens, les enregistrements peuvent être conservés jusqu'à 100 jours (cf. art. 4 ch. 6 RU).

7. Informations aux collaboratrices et collaborateurs

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

---

[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)

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

En l'état, les collaboratrices et collaborateurs de _____ doivent signer une clause de confidentialité dans la mesure où il s'agit de données sensibles. N'étant pas agent de l'état, ils ne sont pas soumis au secret de fonction. Ce nonobstant, ils restent soumis au secret de confidentialité. Par ailleurs, la clause de confidentialité est annexée au RU.

IV. Conclusion

Dans le cadre de la demande d'installation du système de vidéosurveillance avec enregistrement sis au **Foyer Sainte-Elisabeth**, Route des Botzet 4-6, 1700 Fribourg

par

ORS Service AG, Route du Petit-Moncor 1A, 1752 Villars-sur-Glâne

l'Autorité cantonale de la transparence et de la protection des données émet un préavis **partiellement favorable** à la demande d'installation des **caméras 1 à 6**. En effet, il n'est pas autorisé la vision en temps réel. Toutefois, l'enregistrement paraît nécessaire, **aux conditions suivantes :**

a. but : l'article 1 chiffre 3 du RU est modifié pour ne comprendre que les buts conformes à la LVid : soit la prévention des atteintes aux biens et/ou aux personnes et la contribution à la poursuite et à la répression des infractions.

b. proportionnalité : les horaires précis de vidéosurveillance sont mentionnés à l'article 1 chiffre 4 RU (24h/24, 7j/7 – enregistrement). La vision en temps réel étant refusé, l'écran de la réception est enlevé. La vision en direct est également supprimée des fonctionnalités présentes dans le bureau du responsable. Le RU est modifié, voire précisé, à cet effet.

Un cache ou « bloc noir » pour enlever les véhicules du champ de vision est ajouté à la caméra 2. Les images ne peuvent être utilisées à des fins de contrôle du personnel.

Le système de vidéosurveillance, à la lumière de la proportionnalité, est réévalué dans un délai de trois ans.

c. sécurité des données : 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. En outre, le lieu d'hébergement des données, du serveur local et des back-up, le transfert des données, le mode de transmission des données (câble), le chiffrement des données et la gestion des accès ainsi que l'accès à distance ou non sont précisés dans le RU (cf. art. 5 RU).

d. durée de conservation : la durée de conservation des données est portée à 7 jours maximum hors atteinte et 100 jours maximum en cas d'atteinte avérée.

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

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

g. clause de confidentialité : les collaboratrices et collaborateurs de _____ doivent signer 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 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 PFPDT sur le sujet (cf. https://www.edoeb.admin.ch/datenschutz/00763/00983/00996/index.html?lang=fr), 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 au requérant 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 l'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

—

- formulaire de demande d'autorisation d'installer un système de vidéosurveillance avec enregistrement
- complément du 13 octobre 2020