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 2020-LV-20

PRÉAVIS
du 10 juin 2021

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

Demande d'autorisation d'installation d'un système de vidéosurveillance avec enregistrement sis à la **Résidence Saint-Martin**, Route de la Résidence 5, 1741 Cottens

Résidence Saint-Martin, Route de la Résidence 1, 1741 Cottens

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 alinéa 2 de la Loi cantonale du 7 décembre 2010 sur la vidéosurveillance (LVid ; RSF 17.3) ;
- l'article 5 alinéa 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'article 1 alinéa 1 de l'Ordonnance cantonale du 30 janvier 2018 fixant la liste des établissements médico-sociaux du canton de Fribourg (RSF 834.2.41) ;
- le Code civil suisse du 10 décembre 1907 (CC ; RS 210),

l'Autorité cantonale de la transparence et de la protection des données (ATPrD) formule le présent préavis concernant la requête de la Résidence Saint-Martin (ci-après : la requérante) visant à l'installation d'un système de vidéosurveillance avec enregistrement sis à la Route de la Résidence 5, 1741 Cottens, comprenant 5 caméras de type _____, fixes, fonctionnant sur détection de mouvement 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 3 septembre 2020 ainsi que des compléments de la requérante transmis par la Préfecture de la Sarine par courrier du 16 mars 2021.

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 (art. 2 al. 2 let. b LVid). La Résidence Saint-Martin est au bénéfice d'une reconnaissance de l'État. Au vu des informations présentes au dossier, les caméras capturent des images de la piscine, de l'entrée du

vestiaire et du fitness de la requérante. 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 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 d'« assurer la sécurité des usagers de la piscine et du fitness, situés dans le bâtiment Archipel, route de la Résidence 5, à 1741 Cottens. Ce système se veut dissuasif, pour éviter toutes déprédations ou vols, mais aussi apporter les éléments nécessaires à tout incident ou accident qui pourraient parvenir » (art. 1 du Règlement d'utilisation ; ci-après : RU).

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

1) assurer la sécurité des usagers de la piscine et du fitness ;
2) éviter toute déprédation ou vol ;
3) apporter les éléments nécessaires à tout incident ou accident qui pourrait parvenir.

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

1.1 Quant à l'analyse des risques

Il s'agit de déterminer s'il peut y avoir des atteintes contre des personnes ou des biens dans les lieux à protéger ou s'il y a un danger concret que des atteintes se produisent. Il ressort du dossier que l'analyse s'axe principalement autour de dangers dus à l'âge des résident-e-s et aux particularités des lieux (chute dans les escaliers, glissades sur les sols mouillés de la piscine, noyade suite à un malaise, etc.). Quoique la demande fasse état d'une volonté d'éviter toute déprédation et/ou vol, le dossier ne mentionne aucun dépôt de plainte, aucune déprédation constatée, ni un quelconque dommage enregistré.

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 la requérante est consciente des risques et envisage d'y remédier (installation de sols antidérapants, information aux résidents, mise en place de trousses de premier secours à proximité, installation de capteurs et alarmes, etc.). Néanmoins, aucune information quant à la présence de surveillant-e-s n'a été apportée. Il est vrai qu'avec une piscine, il est indéniable que la Résidence bénéficie d'une présence continue, voire d'un-e ou plusieurs surveillant-e-s sur place. Seule la présence d'un maître-nageur (sans précision de son horaire), en tant qu'utilisateur avec accès à la vision en direct, est portée à notre connaissance.

La requérante n'apporte cependant aucune précision quant à l'appréciation faite suite aux différentes mesures apportées qui justifierait l'installation d'une vidéosurveillance. Certes, l'analyse des risques s'arrête sur les lieux de pose, offre des mesures à prendre et présente également celles déjà prises ; ce nonobstant, elle ne soulève nullement les raisons propres à la vidéosurveillance.

1.3 Quant au but

Comme mentionné au point II. 1, le but du présent système est d'« assurer la sécurité des usagers de la piscine et du fitness, situés dans le bâtiment Archipel, route de la Résidence 5, à 1741 Cottens. Ce système se veut dissuasif, pour éviter toutes déprédations ou vols, mais aussi apporter les éléments nécessaires à tout incident ou accident qui pourraient parvenir ». Dès lors, le système (*cf*. RU) prévoit de poursuivre trois buts : assurer la sécurité des usagers de la piscine et du fitness, éviter toute déprédation ou vol et apporter les éléments nécessaires à tout incident ou accident qui pourrait parvenir.

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 susmentionnés semblent entrer 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. Mais, au vu de la formulation du RU, l'Autorité recommande la tournure suivante : « le but est de prévenir toutes atteintes aux personnes et aux usagers de la piscine et du fitness, situés dans le bâtiment Archipel, route de la Résidence 5, à 1741 Cottens. Ce système se veut dissuasif, pour éviter toutes déprédations ou vols, mais aussi contribuer à la poursuite et à la répression d'infractions ». 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 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 de ses données personnelles (art. 12 al. 2 Cst) ainsi que 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 propre 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 envisageables. Il

est indéniable que des alternatives efficaces à la vidéosurveillance existent, sans pour autant remettre en question la nécessité de celle-ci (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 (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 (TC FR 601 2014 46 du 20 août 2015, consid. 2b/cc). En l'état, on peut admettre que l'installation d'un système de vidéosurveillance à la Résidence St-Martin 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.

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. 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 5** : enregistrement et vision en temps réel.

  Lorsqu'un enregistrement est doublé d'une vision directe, l'atteinte est considérée comme particulièrement grave (FLÜCKIGER/AUER, op. cit., p. 934).

  Le tableau nommé « Liste des caméras » mentionne que les images sont uniquement visionnées en cas de problème. Cela ~~se comprend~~ concerne uniquement l'enregistrement. Cela étant, il ressort des documents que le maître-nageur a un accès pour la vision en direct. À défaut de précision, l'Autorité part de l'idée que la vision en direct s'étend sur l'ensemble des caméras. Le personnel, les résident-e-s et les visiteurs doivent être informé-e-s de l'enregistrement ainsi que de la vision en direct ;

Camera 1 – piscine – enregistrement des images et vision en temps réel.

Au vu du risque important que peuvent présenter la noyade, les malaises, etc., l'Autorité est favorable non seulement à l'enregistrement, mais également à la vision en temps réel. Ce nonobstant, l'enregistrement 24h/24 se justifie, alors que la vision en temps réel n'a de sens qu'en présence du maître-nageur. Partant, cette fonctionnalité est tributaire de l'horaire de présence de celui-ci. Partant, l'horaire de présence du maître-nageur doit être renseigné et la vision en temps réel coordonnée avec celui-ci.

Camera 2 – piscine – enregistrement des images et vision en temps réel.

Il est renvoyé à l'argumentation de la caméra 1 ;

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

Le champ de vision permet de voir l'intérieur des vestiaires et notamment les résident-e-s en sous-vêtements, voire nu-e-s. Partant, ni l'enregistrement ni la vision en temps réel ne sont justifiés.

Pour autant que le champ de vision soit modifié, voire un cache ou bloque noir soit mis en en place, seuls l'enregistrement est envisageable. La vision en direct par le maître-nageur n'a, à cet endroit (vestiaire fitness), aucune raison d'être.

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

Au vu de l'âge des résidents, un fitness peut présenter des risques. À notre sens, la présence de surveillant-e-s est indispensable et limite le besoin de vidéosurveillance. À tout le moins, en dehors des heures d'ouverture, l'enregistrement est envisageable. La vision en temps réel ne souffre pas l'examen de la proportionnalité, à défaut d'information plus détaillée, ce d'autant qu'elle est proposée pour le maître-nageur.

Camera 5 – fitness – enregistrement des images et vision en temps réel.

Il est renvoyé à l'argumentation de la caméra 4.

Dès lors que la vision en direct dépend de la présence du maître-nageur, l'horaire de présence de celui-ci doit être renseigné. Les informations sont ajoutées dans le RU (art. 4 RU). Les horaires doivent être portés à la connaissance de la Préfecture pour appréciation définitive à la lumière du principe de la proportionnalité.

Il ressort du dossier que la Direction, le comptable, le comptable 2 et le maître-nageur ont accès aux images. Il semble disproportionné que ce nombre de personnes ait accès aux images. La nécessité pour les comptables est d'autant plus douteuse, en l'absence d'une motivation y relative. Il sied en outre de relever qu'il n'est pas spécifié le nombre de membres qui compose la Direction. En ce sens, il se justifie de restreindre l'accès à deux, voire trois personnes maximum. Cette information doit être ajoutée dans le RU.

Par ailleurs, il importe de préciser l'accès des personnes autorisées dans le RU. Ainsi seul le maître-nageur bénéficie d'un accès en direct. Il n'a toutefois aucun accès aux enregistrements, à la différence des personnes autorisées au sein de la Direction. Ces dernières n'ont toutefois pas d'accès aux images en direct. Le RU est modifié en ce sens.

Une réévaluation doit 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. 8 RU). Ce nonobstant, l'information n'est pas complète. Ainsi l'article a la tournure 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 ». Cela étant, l'information doit être suffisante pour les cas de surveillance en temps réel (notamment pour les visiteurs).

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)

Le RU est lacunaire sur nombre de points. Premièrement, l'organe responsable du système de vidéosurveillance doit être renseigné. La Direction de la Résidence St-Martin est l'organe responsable. Cette information doit être mentionnée dans le RU. Deuxièmement, concernant les personnes autorisées, celles-ci sont désignées par leur fonction dans le RU (2 à 3 maximum). Il est en outre spécifié le type d'accès autorisé (*cf.* chap. III, ch. 2, p. 5). Ainsi que les personnes autorisées sont soumises à l'obligation du respect du secret de fonction, respectivement de confidentialité. Troisièmement, concernant la localisation des serveurs centraux (notamment de l'installateur) et du serveur local (normalement armoire fermée à clé dans un local sur site de la requérante) ainsi que l'hébergement des données, des précisions sont nécessaires. Il est nécessaire de spécifier le mode de transmission (wifi, câble, etc.), le chiffrement du stockage et/ou le transfert de données ainsi que le détenteur de la clé de chiffrement qui doit être en main de l'organe responsable. En outre, l'article 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 (à accéder aux enregistrements) ont accès au serveur local. Par surabondance, la question de la sous-traitance se pose, à savoir si la requérante 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 effet, la requérante reste soumise à la LPrD (art. 2 al. 1 let. b LPrD ; art. 1 al. 2 LVid), et notamment aux articles 12*b* ss LPrD.

« Concernant la sécurité des données, le RU peut mentionner ce qui suit :

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. xx) ;*
   - *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 du Foyer.*

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 6 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 enregistrées et visionnées en direct ; et d'un chiffre expliquant que toute fonctionnalité permettant d'émettre et/ou enregistrer des sons n'est pas autorisée.

« Les chiffres ou articles modifiés et/ou ajoutés du RU peuvent prendre la tournure suivante :

1. *Les données enregistrées ne sont utilisées que dans le cadre du but défini à l'article 2.*

2. *Les titulaires d'autorisation personnelle 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 enregistrées et visionnées en temps réel.*

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 proposée est trop longue (art. 9 RU). Au vu de l'analyse des risques, 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 » (*cf.* 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 la protection. Partant, les données doivent être détruites après 7 jours (automatiquement). En cas d'atteintes avérées aux personnes ou aux biens, les enregistrements peuvent être conservés jusqu'à 100 jours. Le RU est modifié en 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 informé-e-s 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 et consentement

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

En effet, quand bien même le secret de fonction s'applique au fonctionnaire de l'État, 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 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

[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).

l'administration publique, AJP/PJA 6/2019, p. 609 ss, p. 613 s.). La clause de confidentialité est annexée au RU.

En outre, la requérante reste soumise aux règles spécifiques du CC en matière de protection de l'adulte et protection de la personnalité. Afin d'être conforme à la législation, le ou la résident-e, respectivement son représentant légal, doit être informé-e et avoir consenti au système de vidéosurveillance (par ana. ATF 142 III 263, JdT 2017 II 423, consid. 2.2.2 et réf. citées).

IV. Conclusion

Dans le cadre de la demande d'installation du système de vidéosurveillance avec enregistrement sis à la **Résidence Saint-Martin**, Route de la Résidence 5, 1741 Cottens

par

Résidence Saint-Martin, Route de la Résidence 1, 1741 Cottens

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

- **favorable** à la demande d'installation des **caméras 1 et 2** ;
- **partiellement favorable** à la demande d'installation des **caméras 4 à 5**. En effet, il n'est pas autorisé la vision en temps réel. Toutefois, l'enregistrement paraît nécessaire ;
- **défavorable** à la demande d'installation de la **caméra 3**.

aux conditions suivantes :

a. but : l'article 1 RU est formulé dans les sens des recommandations ci-dessus (*cf.* chap. II, ch. 1.3).

b. analyse des risques et des moyens de prévention : une réévaluation du système de vidéosurveillance, à la lumière de la proportionnalité, doit être opérée dans un délai de trois ans concernant notamment les risques d'atteinte et la portée de la mesure.

c. proportionnalité : les personnes autorisées sont au nombre de 3 maximum. L'enregistrement de la caméra 4 est compris en dehors des horaires de présence du ou de la surveillant-e. L'horaire de présence du maître-nageur, voire des surveillant-e-s, est ajouté dans le RU (art. 4 RU).

d. Signalement : la formule suivante est favorisée : « le système de vidéosurveillance est signalé à ses abords au moyen de panneaux informant sans équivoque les personnes se trouvant dans la zone surveillée (p. ex. sous la forme d'un pictogramme) et mentionnant le responsable du système ».

e. sécurité des données : le RU est complété sur les points suivants : la Direction de la Résidence St-Martin est l'organe responsable (art. 7 RU) ; les personnes autorisées sont désignées par leur fonction dans le RU (2 à 3 maximum). Il est en outre spécifié le type d'accès autorisé (enregistrement ou vision en direct, *cf.* chap. III, ch. 2, p. 5) et il est indiqué que celles-ci sont soumises à l'obligation de respecter le secret de fonction, respectivement de confidentialité ; la localisation des serveurs et l'hébergement des données ; la localisation des serveurs centraux (notamment de l'installateur) ainsi que celle du serveur local (normalement armoire fermé à clé dans un local sur site de la requérante) ; le mode de transmission ; le stockage des enregistrements 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 (à accéder aux

enregistrements) ont accès au serveur local ; la sous-traitance ; le chiffrement des données et la mention que la clé de chiffrement est en main de l'organe responsable ; l'obligation pour les utilisateurs de changer régulièrement le mot de passe ; etc. Il est pour le surplus renvoyé ci-dessus (*cf.* chap. III, ch. 5, p. 6 s.).

f. *destruction des images* : l'article 9 RU déclare qu'il incombe aux responsables de s'informer régulièrement de la situation à la Résidence St-Martin. Ainsi les données enregistrées sont détruites après 7 jours. En cas d'atteinte avérées aux personnes et/ou aux biens, les enregistrements peuvent être conservées jusqu'à 100 jours.

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

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

i. *clause de confidentialité :* le prestataire mandaté – 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 que si elle filme ses employé-e-s, 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 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 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
- compléments envoyés par requérante