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 70
www.fr.ch/atprd

Réf. : FH/nk 2019-LV-6

PRÉAVIS
du 21 avril 2020

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 Route Jo Siffert 2-4-6, 1762 Givisiez

SAPCO SA, Case postale 1414, 1701 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 4 avril 1972 sur le domaine public (LDP ; RSF 750.1),

l'Autorité cantonale de la transparence et de la protection des données (ATPrD) formule le présent préavis concernant la requête de SAPCO SA (ci-après : la requérante) visant à l'installation d'un système de vidéosurveillance avec enregistrement, sis route Jo Siffert 2-4-6, comprenant 2 caméras de type _____, fixe, communication WiFi entre les deux caméras, possibilité de zoom, fonctionnant 24h/24.

Ce préavis se base sur les éléments qui ressortent du formulaire de demande d'autorisation d'installation d'un système de vidéosurveillance avec enregistrement daté du 1er mars 2019, du Règlement d'utilisation et des annexes transmis par la Préfecture de la Sarine par courrier du 20 mars 2019 ; de la vision locale du 14 janvier 2020 ainsi que des compléments transmis par courrier des 27 janvier et 4 février 2020 par la requérante. 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). Aux termes de l'article 3 alinéa 1 chiffre 3 LDP, les routes cantonales appartiennent au domaine public. Au vu des informations fournies par la requérante, les deux caméras capturent des images de la route cantonale de Belfaux à Givisiez. 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. Nous examinons d'abord l'analyse des risques (cf. chap. II), ensuite le respect des principes généraux et autres conditions légales, 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 et la durée de conservation des images (cf. chap. III, ch. 1 à 6).

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 les actes de vandalisme et de déprédation et d'identifier les personnes ayant commis de tels actes dans le parking (niveau rez inférieur) » (cf. art. 1 ch. 3 du Règlement ; ci-après : RU).

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. Lors de la vision locale du 14 janvier 2020, la requérant a expliqué que les barrières automatiques aux entrées (et respectivement aux sorties) subissent plus d'une quinzaine de fois par année des dommages. Celles-ci sont enlevées de leurs socles ou casser par les personnes désireuses de ne pas s'acquitter du paiement du stationnement. Au vu de ce qui précède, des atteintes aux biens sont relevées.

1.2 Quant aux moyens

Il s'agit de déterminer quels sont les moyens actuels et quels seraient les moyens possibles et moins radicaux que la vidéosurveillance. La requérante ne dispose pas d'agent de sécurité sur place. Seuls le responsable technique (conciergerie) et son suppléant sont amenés à intervenir en cas de besoin ; soit de manière ponctuelle. En l'espèce, pour prévenir les atteintes aux biens, la vidéosurveillance semble être un moyen efficace.

1.3 Quant au but

Comme mentionné au point II. 1, le but du présent système est « de prévenir les actes de vandalisme et de déprédation et d'identifier les personnes ayant commis de tels actes dans le parking (niveau rez inférieur) ». Dès lors, il paraît envisageable que le moyen prôné permette d'atteindre le but poursuivi et limite les risques cités plus haut.

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 proximité de barrières automatiques est apte à limiter les atteintes aux personnes et aux biens et peut comporter un effet dissuasif.

Pour être proportionnée, la vidéosurveillance ne peut être installée qu'aux endroits où elle s'avère nécessaire, c'est-à-dire dans les lieux où l'intérêt public visé ne parvient pas à être atteint par d'autres moyens (FLÜCKIGER/AUER, op. cit., p. 938). Concrètement, la vidéosurveillance doit se limiter aux endroits où, selon l'expérience, se déroulent plus fréquemment des actes de vandalisme et dans lesquels règne par conséquent un plus grand sentiment d'insécurité. Le principe de la proportionnalité s'oppose à une vidéosurveillance généralisée de tout le territoire sans tenir compte du niveau d'insécurité qui y règne (FLÜCKIGER/AUER, op. cit., p. 938). En l'espèce, la vidéosurveillance aux entrées pourvues en barrières automatiques est conforme au respect du principe.

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, les deux caméras enregistrent les images qui peuvent également être visionnées en temps réel (cf. Tableau des caméras). Le fait d'enregistrer les images et de les visionner en direct porte une atteinte plus grande à la personnalité des personnes concernées. Partant, pour être conforme à la protection des données, les écrans de visualisation doivent être dirigés de manière à ce qu'aucune personne non-autorisée ne puisse les visionner en direct (p. ex. : orienter face à un mur). Si la visualisation devait se faire par le biais d'un appareil privé (tel que Ipad, smartphone ou ordinateur privé), des mesures de sécurité doivent être mises en place par le responsable IT (antivirus, accès avec authentification forte, pas d'enregistrement et téléchargement de l'image dans l'appareil privé, journalisation, etc.). Ce nonobstant, un système de floutage des images devrait être mis en place afin de réduire au maximum l'atteinte aux libertés des personnes filmées. En effet, un tel système brouille automatiquement les visages entrant dans le champ de vision de la caméra et empêche une reconnaissance immédiate de leur identité. Ce n'est qu'en cas

d'infractions avérées que le floutage peut être ponctuellement désactivé afin de dévoiler l'identité du responsable (cf. Arrêt TC FR 601 2014 46, consid. 3b).

Afin d'avoir une vue générale, chaque caméra sera analysée sous l'angle de la proportionnalité :

- **Camera 1 – enregistrement des images et vision en temps réel**. Il sied de rappeler que lorsqu'un enregistrement est doublé d'une vision directe, l'atteinte est considérée comme particulièrement grave. En l'espèce, l'absence d'agents de sécurité sur le site admet la vision en direct. Bien que la signalisation de la présence d'un système de vidéosurveillance bénéficie d'un effet dissuasif, une vision en direct peut se justifier aux entrées et sorties. Partant, la caméra respecte le principe de la proportionnalité. Les usagers doivent être informés de la vision en direct ;

- **Camera 2 – enregistrement des images et vision en temps réel**. Il sied de rappeler que lorsqu'un enregistrement est doublé d'une vision directe, l'atteinte est considérée comme particulièrement grave. En l'espèce, l'absence d'agents de sécurité sur le site admet la vision en direct. Bien que la signalisation de la présence d'un système de vidéosurveillance bénéficie d'un effet dissuasif, une vision en direct peut se justifier aux entrées et sorties. Partant, la caméra respecte le principe de la proportionnalité. Les usagers doivent être informés de la vision en direct.

Il est important de limiter les zones soumises à la vidéosurveillance, il convient de veiller à ce que les caméras ne filment que les barrières. Les immeubles d'habitation et autres propriétés privées n'ont pas à être filmés. Partant, la présence des blocs noirs (cf. Tableau des caméras) veille au respect de la législation.

L'article 4 RU est complété d'un chiffre distinguant les enregistrements continus standard des enregistrements faisant suite à une extraction de données ; d'un chiffre expliquant que les images sont enregistrées et visionnées en direct (cf. Tableau des caméras) ; et d'un chiffre expliquant que toute fonctionnalité permettant d'émettre et/ou enregistrer des sons n'est pas autorisée.

3. Signalement adéquat du système (art. 4 al. 1 let. b LVid)

Des documents à disposition, il ne ressort pas que l'information est prévue. Ainsi, il s'agira de compléter le Règlement d'utilisation en y ajoutant un article à cet effet, dont la teneur sera la suivante : « Le système de surveillance 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 ». En outre, l'information doit être suffisante pour les cas de surveillance en temps réel.

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)

L'article 5 RU est complété et propose une différence entre l'enregistrement en continu standard et l'enregistrement faisant suite à une extraction pour atteinte avérée. Le stockage offre une distinction semblable. Le stockage ainsi que le transfert des données doivent être chiffrés. La clé de chiffrement reste uniquement en main du responsable IT.

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

Les durées de conservation envisagées sont conformes à la législation en vigueur.

7. Information aux collaboratrices et collaborateurs

La requérante est rendue attentive au fait que, dans la mesure où elle filme ses employés, ces derniers doivent être informés des endroits sous vidéosurveillance et des horaires où le système fonctionne. En outre, l'ensemble du personnel travaillant dans le bâtiment doit également être informé.

8. Droit d'accès (art. 1 al. 2 *in fine* LVid ; art. 23 LPrD)

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 (p. ex., en les floutant). Un article relatif au droit d'accès est ajouté dans le RU.

9. Clause de confidentialité

Les personnes autorisées à consulter les images (cf. art. 2 al. 2 RU et Tableau des caméras) ne sont pas soumises au secret de fonction n'étant pas des fonctionnaires de l'État. Dans la mesure où il s'agit de données sensibles et soumises au secret de fonction, ils doivent signer une clause de confidentialité, réservant des suites juridiques en cas de non-respect. Celle-ci est annexée au RU.

IV. Conclusion

Dans le cadre de la demande d'installation du système de vidéosurveillance avec enregistrement sis route Route Jo Siffert 2-4-6, 1762 Givisiez

par

SAPCO SA, Case postale 1414, 1701 Fribourg

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

- préavis **favorable** à la demande d'installation des deux **caméras** avec enregistrement ;

aux conditions suivantes :

a. *proportionnalité :* la présence des blocs noirs sur l'image est maintenue, sous réserve des cas d'atteinte avérée. L'article 4 RU est complété d'un chiffre distinguant les enregistrements continus standard des enregistrements faisant suite à une extraction de données ; d'un chiffre expliquant que les images sont enregistrées et visionnées en direct (cf. Tableau des caméras) ; et d'un chiffre expliquant que toute fonctionnalité permettant d'émettre et/ou enregistrer des sons n'est pas autorisée.

b. *signalement* : un article relatif au signalement du système de surveillance est ajouté.

c. *sécurité des données* : l'article 5 RU est complété d'un chiffre différenciant l'enregistrement en continu standard de l'enregistrement faisant suite à une extraction pour atteinte avérée. Le stockage offre une distinction semblable. Le stockage ainsi que le transfert des données doivent être chiffrés. La clé de chiffrement reste uniquement en main du responsable IT. L'article 5 RU est modifié en conséquence. Le responsable IT s'assure des mesures organisationnelles et techniques concernant l'accès des personnes autorisées aux enregistrements, notamment s'agissant des appareils utilisés.

d. *information aux collaboratrices et collaborateurs* : les collaboratrices et collaborateurs sont informés des endroits sous vidéosurveillance et des horaires où le système fonctionne. Ils doivent cependant être particulièrement rendus attentifs à la présence de caméras dans les parkings où des informations non-nécessaires au but de la vidéosurveillance peuvent être enregistrées (personnes accompagnantes, etc.). En outre, l'ensemble du personnel travaillant dans le bâtiment est également informé.

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

f. *clause de confidentialité :* l'article 2 chiffre 2, 2ème paragraphe, RU est modifiée dès lors que les personnes autorisées ne sont pas soumis au secret de fonction n'étant pas des fonctionnaires de l'État. Dans la mesure où il s'agit de données sensibles et soumises au secret de fonction, ils doivent signer une clause de confidentialité, réservant des suites juridiques en cas de non-respect. Celle-ci est annexée au RU.

Vu le défaut d'informations susmentionnées, l'Autorité octroie une validation de principe. Toutefois, le RU est complété en ce sens (point a à f) et doit être transmis à la Préfecture ainsi qu'à l'Autorité pour approbation définitive.

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 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 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
—
- formulaires de demande d'autorisation d'installer un système de vidéosurveillance avec enregistrement
- dossier en retour