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-2

PRÉAVIS
du 15 octobre 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 sise Route du Château-d'Affry 40*b* et 46, 1762 Givisiez

p.a. Commune de Givisiez, Place d'Affry 1, Case postale, 1762 Givisiez

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) ;
- la Loi cantonale du 25 septembre 1980 sur les communes (LCo ; RSF 140.1) ;
- la Loi cantonale du 4 avril 1972 sur le domaine public (LDP ; RSF 750.1) ;
- l'article 3 alinéa 1 lettre a du Règlement général de police des communes membres de l'Association pour l'exploitation d'un corps de police intercommunale (ACoPol),

l'Autorité cantonale de la transparence et de la protection des données (ATPrD) formule le présent préavis concernant la requête de la Commune de Givisiez (ci-après : la requérante) visant à l'installation d'un système de vidéosurveillance avec enregistrement, sis route du Château-d'Affry 40b et route du Château-d'Affry 46, 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 21 janvier 2019, du Règlement d'utilisation, des annexes, des avis de dégâts et dépôts de plainte pénale joints, transmis par la Préfecture de la Sarine par courrier du 28 janvier 2019 ; de la vision locale du 14 janvier 2020 ainsi que des compléments transmis par la requérante par courriels des 24 janvier et 5 février 2020. 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 2 chiffre 2 LDP, les routes communales appartiennent au domaine public. Au vu des informations fournies par la

requérante, les deux caméras capturent chacune des images d'une route communale : la barrière sise à la route du Château-d'Affry 40*b* ainsi que la barrière sise à la route du Château-d'Affry 46. Partant, la vidéosurveillance au moyen de caméras dôme, dont le champ de vision couvre tout ou partie de lieux publics, 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, la durée de conservation des images, le droit d'accès et le respect de la confidentialité (cf. chap. III, ch. 1 à 8).

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 au patrimoine communal » (cf. art. 1 ch. 3 du Règlement d'utilisation ; ci-après : RU).

Une analyse des risques, à la lumière du principe de la proportionnalité, ne figure pas au dossier. Cela étant, sur la base de la vision locale du 14 janvier 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 de nombreux dégâts ont été à multiples reprises constatés et dénoncés à la police cantonale. Depuis 2018, il y a eu près de 20 cas de dommages dont seuls sept auteurs se sont spontanément dénoncés. Dans la plupart des cas, des plaintes contre inconnu ont été déposées. Le dossier fait état de photographies permettant d'apprécier les dommages causés aux barrières. Le montant (total) des dommages reste encore à déterminer. Au vu de ce qui précède, les zones à surveiller (art. 1 ch. 5, 4ème tiret RU) peuvent être désignées comme à risque.

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. Les barrières de la route du Château-d'Affry ne disposent d'aucun matériel de surveillance. En outre, des dommages ont été constatés. En l'espèce, pour prévenir les atteintes aux biens communaux, la vidéosurveillance semble être un moyen efficace.

1.3 Quant au but

Comme mentionné au point II. 1, le but du présent système est « la prévention des actes de vandalisme et l'identification des personnes ayant causé des dégâts au patrimoine communal ». 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 des barrières de la route du Château-d'Affry est apte à limiter les atteintes aux biens et peut comporter un effet dissuasif.

Le principe de la proportionnalité ne s'applique pas seulement à la surveillance elle-même, mais également au dispositif technique choisi (Message n° 202 du Conseil d'Etat du 6 juillet 2010 accompagnant le projet de loi sur la vidéosurveillance, 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. Il ne ressort, toutefois, pas de la demande que les images soient visionnées en temps réel. Ainsi, nous partons du principe que les enregistrements sont uniquement consultés en cas d'atteinte avérée.

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

- **Camera barrière – Route du Château-d'Affry 40b : enregistrement des images. Il n'y a pas de vision en temps réel**. La caméra respecte le principe de la proportionnalité ;

- **Camera barrière – Route du Château-d'Affry 46 : enregistrement des images. Il n'y a pas de vision en temps réel**. La caméra respecte le principe de la proportionnalité ;

Il est important de limiter les zones soumises à la vidéosurveillance. Il convient de veiller à ce que les caméras ne filment que la route et les barrières. Les immeubles d'habitation et autres propriétés privées ne doivent pas être filmés. Partant, le champ de la vidéosurveillance tel que présenté dans le dossier n'est pas conforme, de sorte que des masques noirs doivent être ajoutés aux prises de vue des caméras. Les champs de vision adaptés ainsi que le RU modifié doivent être communiqués à la Préfecture.

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 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. *[..*
2. *...]*
3. *Les données enregistrées sont automatiquement détruites après 72 heures. En cas d'atteinte aux aux biens, les données enregistrées sont extraites sur un support informatique 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.
4. *Des copies ou impressions peuvent être effectuées mais doivent être détruites dans les mêmes délais que les originaux. Un protocole de copie est conservé.*
5. *Les images sont uniquement enregistrées et visionnées par les personnes autorisées (cf. art. 2 ch. 2).*
6. *Toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons n'est pas autorisée.*
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).*

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

Des documents à disposition, il ne ressort pas que l'information soit prévue. Ainsi, il s'agira de compléter le RU en y ajoutant un chiffre 8 à l'article 1, avec la mention « 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. 1 ch. 3 RU), sous réserve de l'adaptation des champs de vision.

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

L'accès accordé à l'ensemble des agents assermentés de l'ACoPol est à notre sens trop large (cf. art. 2 ch. 2 RU), dans la mesure où l'accès à ces données sensibles par un ou deux membres de l'ACoPol paraît suffisant. En effet, seules les personnes pour lesquelles un accès est nécessaire en raison de leur

fonction ou leur tâche peuvent figurer sur la liste des personnes autorisées. Dès lors, les personnes autorisées sont au nombre de deux ou trois et doivent être mentionnées dans un tableau annexé au RU.

Les chiffres modifiés et/ou ajoutés de l'article 2 RU peuvent prendre la tournure suivante :

1. *[…]*
2. *Les personnes autorisées à consulter les données enregistrées par le système de vidéosurveillance sont les personnes mentionnées à l'Annexe 1 du RU ;*
3. *Ces personnes sont soumises au secret de fonction, respectivement aux règles de confidentialité.*

À ce sujet, un renvoi à l'article 2 chiffre 2 RU est introduit à l'article 5 chiffre 1, 1er tiret. Le RU est modifié dans ce sens. En outre, l'article 5 RU est complété d'un chiffre distinguant les enregistrements continus standard (72 heures ; cf. point 6 ci-dessous) des enregistrements faisant suite à une extraction de données (100 jours ; cf. point 6 ci-dessous) ;

Le système de vidéosurveillance se trouve sur un réseau isolé. Un accès (protégé par mot de passe) est autorisé depuis Internet. Il s'agit ici de préciser à l'article 5 du RU que seules les personnes autorisées (cf. art. 2 ch. 2 RU) ont accès au mot de passe.

Les enregistrements sont hébergés dans le bâtiment de l'administration communale, sur un serveur qui lui est réservé. Le stockage ainsi que le transfert des données doivent être chiffrés ou cryptés. La clé de chiffrement est en main de l'organe responsable. En outre, aucun accès aux données par les employés de _____ ne peut pas être autorisé, notamment en rapport avec la maintenance de l'installation. Le RU est modifié dans ce sens.

La vision en temps réel n'ayant pas été requise, cette fonctionnalité ne peut être maintenue. Elle doit être retirée des possibilités techniques des administrateurs.

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 (mot de passe) est délivrée aux personnes autorisées (cf. art. 2 ch. 2) ;*
     - *les titulaires d'autorisation personnelle 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.*
   - *un journal des accès est imprimé chaque mois. Il est conservé une année au moins, sous clé, dans le bureau du chef de l'ACoPol. Le journal d'accès est transmis mensuellement à l'organe de contrôle interne défini à l'article 6a.*
   - *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 (serveur de stockage propre) et d'hébergement des données (et/ou la back-up) sont protégés dans un bâtiment de l'administration communale, fermé à clé et non-accessible aux personnes non-autorisées.*
4. *Le transfert ainsi que le stockage des données sont chiffrés et les clés de chiffrement sont en main de l'organe responsable.*

5. *Les données enregistrées et celles extraites doivent être stockées sur un support physique indépendant, sans accès à distance possible et, sont remises, le cas échéant, au procureur ou au juge en charge de la procédure.*

6. *L'organe responsable s'assure des mesure techniques et organisationnelles concernant l'accès des personnes autorisées aux enregistrements et aux extractions, notamment s'agissant des appareils utilisés.*

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

La durée de conservation proposée est trop longue (cf. art. 4 ch. 3 RU). 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 (cf. https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/technologien/videoueberwachung/explications-sur-la-videosurveillance-sur-le-lieu-de-travail.html). Partant, les données enregistrées devront être détruites après 72 heures. L'article 4 chiffre 3 RU doit être modifié en ce sens. En cas d'atteintes avérées aux biens, les enregistrements peuvent être conservés jusqu'à 100 jours (cf. art. 4 ch. 3 RU).

7. 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 (en les floutant par exemple). Un article relatif au droit d'accès est ajouté dans le RU.

8. Clause de confidentialité

Les collaboratrices et/ou collaborateurs de ACoPol 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, la clause de confidentialité doit faire référence à l'obligation du secret de fonction pour les collaboratrices et/ou collaborateurs de ACoPol. Celles-ci sont annexées au RU.

9. Mesures de contrôles

Les contrôles délégués à des tiers doivent faire l'objet d'un contrat mentionnant les instructions nécessaires au respect du RU et la clause de confidentialité. Cette délégation doit être approuvée préalablement par l'organe responsable.

IV. Conclusion

Dans le cadre de la demande d'installation du système de vidéosurveillance avec enregistrement sis route du Château-d'Affry 40b et route du Château-d'Affry 46

par

la Commune de Givisiez, Place d'Affry 1, Case postale, 1762 Givisiez

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

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

aux conditions suivantes :

a. *proportionnalité :* la présence de blocs noirs sur l'image est mise en place et le champ de vision ne couvre que la route et les barrières. 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 uniquement enregistrées ; et d'un chiffre expliquant que toute fonctionnalité permettant d'émettre et/ou enregistrer des sons n'est pas autorisée.

b. *signalement* : le système de vidéosurveillance est signalé à ses abords au moyen de panneaux informant sans équivoque les personnes se trouvant dans la zone surveillée et mentionnant le responsable du système, par exemple sous forme de pictogramme. Un chiffre 8 à l'article 1 du RU est ajouté dans ce sens.

c. *sécurité des données* : Le nombre de personnes autorisées est restreint à deux ou trois personnes. L'article 2 chiffre 2 RU est modifié en ce sens. Un renvoi vers cette disposition est introduit à l'article 5 chiffre 1, 1er tiret RU. La localisation de l'hébergement, le chiffrement du stockage et/ou des transferts de données, la mention de la clé de chiffrement en main de l'organe responsable, l'obligation du changement régulier du login des administrateurs font l'objet de nouveaux chiffres à l'article 5. La possibilité pour les personnes autorisées d'avoir accès à la vision en temps réel est supprimée. Aucun accès aux données par les employés de _____ n'est autorisé.

L'article 5 est complété d'un chiffre distinguant les enregistrements continus standard (72 heures) des enregistrements faisant suite à une extraction de données (100 jours) et des droits d'accès et mot de passe y relatifs.

d. *durée de conservation des images* : la durée de conservation est limitée à 72 heures maximum et à 100 jours en cas d'atteinte avérée. L'article 5 RU est modifié dans ce sens.

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 :* les collaboratrices et collaborateurs de ACoPol doivent signer une clause de confidentialité. Celle-ci est annexée au RU.

g. *mesure de contrôle* : les contrôles délégués à des tiers doivent faire l'objet d'un contrat mentionnant les instructions nécessaires au respect du RU et la clause de confidentialité. Cette délégation doit être approuvée préalablement par l'organe responsable.

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

V. Remarques

> 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
—
- formulaires de demande d'autorisation d'installer un système de vidéosurveillance avec enregistrement
- consentement du propriétaire du terrain agricole et ses annexes