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 2021-LV-10

PRÉAVIS
du 16 septembre 2021

À l'attention du Préfet de la Veveyse, M. François Genoud

Demande d'autorisation d'installation d'un système de vidéosurveillance avec enregistrement
sis à l'entrée des WC publics du bâtiment communal, Chemin de la Chapelle 7, 1614 Granges

Commune de Granges, Chemin de la Chapelle 7, 1614 Granges

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 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 la commune de Granges (ci-après : la requérante) visant à l'installation d'un système de vidéosurveillance avec enregistrement, sis à l'entrée des WC extérieurs du bâtiment communal, Chemin de la Chapelle 7, 1614 Granges, comprenant 1 caméra de type _____, avec zoom numérique, fonctionnant 24h/24, 7j/7, sur détection de mouvement.

Ce préavis se base sur les éléments qui ressortent du formulaire de demande d'autorisation d'installation d'un système de vidéosurveillance avec enregistrement daté du 8 février 2021 et de son Règlement d'utilisation, transmis par la Préfecture de la Veveyse par courrier du 15 mars 2021, des premiers compléments transmis par la Préfecture de la Veveyse par courriel du 29 juin 2021 ainsi que le courriel du 12 juillet 2021 de la requérante complétant sa demande.

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). Aux termes de l'article 3 alinéa 2

chiffre 2 LDP, les routes communales appartiennent au domaine public. Sont également des lieux publics, les immeubles ouverts au public qui sont affectés à l'administration publique (art. 2 al. 2 let. b LVid). Au vu des informations fournies par la requérante, la caméra capture une image de l'entrée des WC publics, une partie du bâtiment communal ainsi qu'une partie de la route communale (Chemin de la Chapelle). 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. III), 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. IV, 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'identifier les auteurs de déprédations ou autres actes de vandalisme dans les WC publics extérieurs du bâtiment 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. 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 s'y produisent. Il ressort du dossier que le lieu visé a subi des déprédations à trois reprises, sans qu'il n'ait été possible de déterminer l'auteur des dégâts. Une plainte pénale a été déposée. Le dossier ne mentionne pas dans quel intervalle ni dans quelle tranche horaire ont eu lieu ces actes de vandalisme. Ce nonobstant, il est concevable que des atteintes aux biens puissent survenir.

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 fermeture à clé des WC le soir et le week-end est jugé insatisfaisante par la requérante. Cela étant, aucune information n'est précisée concernant cette appréciation. Toutefois, il semble que d'autres moyens moins incisifs permettraient également de limiter les risques d'atteinte. En effet, la surveillance régulière voire aléatoire par une personne responsable ou par des agents de sécurité permettraient notamment de limiter les atteintes aux biens.

1.3 Quant au but

Comme mentionné au point II. 1, le but du présent système est « d'identifier les auteurs de déprédations ou autres actes de vandalisme dans les WC publics extérieurs du bâtiment communal » (*cf.* art. 1 ch. 3 RU).

Aux termes de l'article 3 alinéa 1 LVid, la vidéosurveillance veille à prévenir les atteintes aux personnes et aux biens et contribue à la poursuite et répression des infractions. Ces deux conditions, soit la prévention des atteintes aux biens et/ou aux personnes et la contribution à la poursuite et à la répression d'infractions, sont cumulatives (TC FR 601 2014 46 du 20 août 2015, consid. 3d)).

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

III. Conditions

1. Exigence de la base légale

L'article 38 Cst prévoit que « toute restriction d'un droit fondamental ou social doit être fondée sur une base légale. Les restrictions graves doivent être prévues par une loi ». En l'occurrence, c'est le cas dans la LVid. En outre, conformément à l'article 4 LPrD (*cf.* art. 1 al. 2 LVid), le traitement de données personnelles ne peut se faire que si une disposition légale le prévoit, ce qui est le cas également.

2. Respect du principe de la proportionnalité (art. 4 al. 1 let. a LVid)

L'article 4 LVid prévoit que les systèmes de vidéosurveillance avec enregistrement sont soumis au respect du principe de la proportionnalité (let. a).

La vidéosurveillance porte atteinte à plusieurs libertés : la liberté personnelle, et plus particulièrement la triple garantie de l'intégrité physique et psychique et de la liberté de mouvement (art. 11 al. 2 Cst), le droit au respect de la sphère privée (art. 12 al. 1 Cst et 8 CEDH), le droit d'être protégé contre l'emploi abusif des données personnelles (art. 12 al. 2 Cst) et la liberté de réunion (art. 24 Cst ; *cf.* FLÜCKIGER/AUER, La vidéosurveillance dans l'œil de la Constitution fédérale, AJP/PJA 2006, p. 931).

Si la mesure paraît apte à atteindre le but visé, il n'en demeure pas moins que la surveillance doit être adéquate, c'est-à-dire apte à atteindre le but visé mais également limitée à ce qui est nécessaire. La surveillance au moyen d'enregistrements vidéo permet la constatation d'infractions en assurant la conservation des preuves et en permettant ainsi un taux d'élucidation élevé. Grâce à l'effet dissuasif qui y est lié, les infractions sont combattues dans un but de maintien de la sécurité et de l'ordre publics (cf. Arrêt TC FR 601 2014 46 du 20 août 2015, consid. 2b/cc). En l'état, on peut dès lors admettre que l'installation des caméras à l'entrée des WC publics 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, la caméra enregistre les images. En outre, la vision en temps réel est possible pour le syndic et la secrétaire. Or, pour que le présent système soit conforme au principe de la proportionnalité, une vidéosurveillance avec enregistrement simple, dont l'enregistrement est effacé automatiquement après une brève durée, n'est pas doublé d'un suivi en temps réel et est visionné ainsi qu'utilisé uniquement en cas de délits avérés, est largement suffisante dans le cas d'espèce. Selon la jurisprudence et les recommandations du Préposé fédéral à la protection des données et à la transparence[1], le dispositif technique utilisé doit également respecter le principe de proportionnalité, notamment en préservant l'anonymat des personnes. En l'occurrence, un système de floutage des images ou des bandes noires devraient être employés afin de réduire au maximum l'atteinte aux libertés des personnes filmées, de sorte que l'installation ne doit filmer que l'entrée des WC publics et non la partie de la route communale. En cas d'infractions avérées, les bandes ou les floutages peuvent être ponctuellement désactivés afin de dévoiler l'identité du responsable (cf. Arrêt TC FR 601 2014 46, consid. 3b). L'efficacité des systèmes de vidéosurveillance n'est ainsi aucunement réduite.

Sous l'angle de la nécessité, des mesures moins incisives seraient envisageables, afin d'atteindre le même but de prévention et de répression des atteintes aux biens. Par exemple, la surveillance régulière voire aléatoire par une personne responsable, du personnel communal ou par des agents de sécurité.

Au sens de la proportionnalité au sens étroit, l'intérêt public à la prévention et à la répression d'infractions (dégâts matériels, atteintes à la personne) doit primer l'intérêt privé au respect des libertés personnelles des personnes (TC FR 601 2014 46, consid. 2b/cc et réf. citées). Nous sommes d'avis que l'intérêt à lutter contre des déprédations des WC publics ne l'emporte pas sur l'atteinte importante au droit de la personnalité des personnes concernées.

Afin de limiter l'atteinte à ce qui est strictement nécessaire, l'entrée des WC n'a pas à être filmée 24h/24h. En effet, une vidéosurveillance, en dehors des horaires d'ouverture de la commune et durant la nuit, soit de 18 heures à 6 heures, semble suffisante ; la présence du personnel communal et des passants permettant de limiter les atteintes.

Au vu de ce qui précède, la vision en temps réel ne passe pas l'examen de la proportionnalité et l'enregistrement ne peut être éventuellement admis que sous un horaire restreint, proportionné aux atteintes et que le champ de vision soit adapté à ce qui est mentionné plus haut. Ainsi, le RU doit être modifié en ce sens. En outre, l'article 4 RU doit également être précisé en distinguant les enregistrements continus standards des enregistrements faisant suite à une extraction de données ; en ajoutant un chiffre expliquant que les images sont uniquement enregistrées.

Au surplus, toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons ne doit pas être utilisée.

Enfin, afin que ce système de surveillance soit toujours conforme aux besoins et aux conditions légales, une réévaluation peut être opérée dans un délai de trois ans concernant notamment les risques d'atteinte et la portée de la mesure.

---

[1] https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/technologien/videoueberwachung/explications-sur-la-videosurveillance-dans-les-vestiaires-et-dan.html)

3. Signalement adéquat du système (art. 4 al. 1 let. b LVid ; art. 8 OVid)

Il ressort des documents à disposition que le signalement prévu est adéquat (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)

Il est rappelé que les utilisateurs devraient changer régulièrement le mot de passe. Une double authentification est recommandée. En outre, seulement en cas d'atteinte avérée, les titulaires d'autorisation personnelle peuvent consulter les images ainsi que les extraire à des fins de poursuite. Ces éléments devraient ressortir clairement du RU.

Concernant l'accès au serveur local ainsi qu'au lieu d'hébergement des enregistrements et/ou d'extraction, seules les personnes autorisées (*cf.* art. 2 al. 2 RU) devraient avoir accès. Le RU est modifié en ce sens.

Concernant la sécurité des données, les informations relatives au fournisseur ou à l'entreprise d'installation et/ou de maintenance (si externalisation) et les mesures techniques (tels que le chiffrement du transfert et du stockage des données, le détenteur des clés, le contrat y relatif) font défaut et devront faire l'objet d'une analyse spécifique.

En cas de sous-traitance, les articles 18 et 12b ss LPrD doivent être respectés. En effet, lorsque l'organe public fait traiter des données par une entreprise externe, des conditions plus strictes doivent être appliquées et doivent être réglées dans un contrat (art. 18 LPrD). Le contrat doit notamment contenir une garantie du niveau adéquat de protection des données ; le lieu du traitement des enregistrements doit être connu et sécurisé ; la durée du contrat ainsi que la durée de conservation des enregistrements doit être fixée ; les modalités de transfert des données du mandataire à la requérante doivent être mises en place ; les responsabilités entre le mandataire et le sous-traitant doivent être réparties ; les modalités selon lesquelles les enregistrements sont sauvegardés, archivés et radiés doivent être décrites avec précision ; des contrôles doivent pourvoir être effectués par la requérante, la Préfecture ainsi que par l'Autorité cantonale de la transparence et de la protection des données, sur les activités du mandataire sous-traitant ; le for de la poursuite ainsi que le droit applicable sont suisses. En outre, les enregistrements doivent être chiffrés au niveau de la transmission et du stockage. Le responsable au sein de la Commune doit être le seul à détenir la clé de cryptage. En effet, le mandataire (qui stocke les enregistrements) ne doit pas pouvoir avoir accès aux données. De plus, la maintenance ne pourra pas être effectuée à distance.

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

Conformément à l'art. 4 al. 1 let. e LVid, les images récoltées par une installation de vidéosurveillance sont conservées pendant trente jours, sauf en cas d'atteintes aux personnes ou aux biens auquel cas le délai peut être porté à cent jours (cf. art. 4 ch. 3 du Règlement d'utilisation). En l'occurrence, comme le but de la vidéosurveillance est limité à « identifier les auteurs de déprédations ou autres actes de vandalisme dans les WC publics extérieurs du bâtiment communal », la conservation des images devrait se limiter à 24h. En effet, selon le Tribunal fédéral, il faut distinguer entre les infractions commises contre des biens et celles commises contre des personnes. Les infractions contre les biens étant

constatées par les autorités étatiques elle-même (et non sur plainte) une longue durée de conservation n'est pas indispensable en cas d'atteinte (cf. ATF 133 I 77 = JdT 2007 I 591). En outre, le Préposé fédéral à la protection des données et à la transparence recommande une durée de conservation de 24 à 72 heures[2]. En effet, les responsables doivent s'informer régulièrement de toute situation pouvant entrer dans le but de la protection. Partant, une durée de conservation de 72 heures paraît suffisante pour permettre à la personne responsable de consulter les enregistrements suite à un délit avéré. Les enregistrements devraient être détruits de manière automatique après les 72 heures. En cas d'atteintes avérées aux personnes ou aux biens, les enregistrements peuvent être extraits et conservés jusqu'à 100 jours. Le RU est modifié en ce sens (cf. art. 4 al. 3 RU).

7. Information aux collaboratrices et collaborateurs

La requérante est rendue attentive au fait que, dans la mesure où elle peut potentiellement filmer ses employés, ces derniers doivent être informés des endroits sous vidéosurveillance et des horaires où le système fonctionne.

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

Un article relatif au droit d'accès est ajouté dans le RU. Celui-ci précise ainsi que « toute personne peut demander au responsable du système l'accès à ses propres données. Le responsable du système répond à la demande tout en respectant les droits de la personnalité des autres personnes concernées (en les floutant par exemple) ».

9. Clause de confidentialité

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

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

IV. Conclusion

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

- **partiellement favorable à la demande d'autorisation d'installation d'un système de vidéosurveillance avec enregistrement** sis à l'entrée des wc publics du bâtiment communal, Chemin de la Chapelle 7 à Granges,

par

l'Administration communale de Granges, **aux conditions suivantes :**

a. proportionnalité : afin de limiter l'atteinte aux droits de la personnalité à ce qui est strictement nécessaire, l'utilisation de la caméra sera limitée à ce qui est nécessaire, soit en dehors des horaires d'ouverture des bureaux communaux et la nuit, soit de 18h00 à 6 heures, à un dispositif de vidéosurveillance avec enregistrement simple pas doublé d'un suivi en temps réel et sera visionné ainsi qu'utilisé uniquement en cas de délits avérés ; le champ de la prise de vue de la caméra devra se limiter à l'entrée des WC publics et ne devra pas être dirigé sur la route communale ; un système de floutage des images devra être employé ; toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons ne doit pas être utilisée ; le système de vidéosurveillance devra être réévalué dans le délai de trois ans afin d'être conforme aux besoins et aux dispositions légales. Le RU sera modifié en ce sens.

b. sécurité des données : en cas de sous-traitance et pour être conforme aux exigences des art. 18 et 12b al. 1 let. b LPrD, un contrat particulier doit être conclu contenant les informations citées plus haut ; les mots de passe doivent être changés régulièrement ; une double authentification est recommandée ; l'accès au serveur local ainsi qu'au lieu d'hébergement des enregistrements et/ou données extraites est réservé aux personnes autorisées (*cf.* art. 2 al. 2 RU). La consultation des images enregistrées peut être effectuée qu'en cas d'atteinte avérée. Les informations relatives au lieu d'hébergement des données, les mesures techniques (chiffrement, détenteur de la clé) font l'objet d'une analyse spécifique ; toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons ne doit pas être utilisée.

c. destruction des images : les données enregistrées sont détruites automatiquement après 72 heures. En cas d'atteinte avérée aux personnes et/ou aux biens, les enregistrements peuvent être extraits et conservées de manière sécurisée jusqu'à 100 jours.

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

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 : le prestataire mandaté 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
- Règlement d'utilisation
- Dossier en retour