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. : RPA/FH 2018-LV-13

PRÉAVIS
du 11 décembre 2018

À l'attention du Préfet de la Gruyère, M. Patrice Borcard

Demande d'autorisation d'installation de vidéosurveillance avec enregistrement sise à la Succursale de l'Office de la circulation et de la navigation, Rue de Planchy 34, 1628 Vuadens

p. a. Office de la circulation et de la navigation, Route de Tavel 10, 1700 Fribourg

I. Généralités

Vu

- les art. 12, 24 et 38 de la Constitution du canton de Fribourg du 16 mai 2004 (Cst ; RSF 10.1) ;
- l'art. 5 al. 2 de la Loi cantonale du 7 décembre 2010 sur la vidéosurveillance (LVid ; RSF 17.3) ;
- l'art. 5 al. 1 de l'Ordonnance cantonale du 23 août 2011 sur la vidéosurveillance (OVid ; RSF 17.31) ;
- la Loi cantonale du 25 novembre 1994 sur la protection des données (LPrD ; RSF 17.1) ;
- le Règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD ; RSF 17.15) ;
- la Loi du 7 mai 1996 sur l'Office de la circulation et de la navigation (LOCN ; RSF 122.23.7),

l'Autorité cantonale de la transparence et de la protection des données (ATPrD) formule le présent préavis concernant la requête de l'Office de la circulation et de la navigation (ci-après : OCN) visant à l'installation d'un système de vidéosurveillance avec enregistrement, sis à sa succursale de Bulle, Rue de Planchy 34, 1628 Vuadens, comprenant 3 caméras dômes de marque Siemens, avec zoom en montage apparent, liaison par câble, enregistrement durant 30 jours au maximum sur un serveur exclusivement dédié aux enregistrements de vidéosurveillance pour le site de Bulle, fonctionnant 7 jours sur 7 et 24 heures sur 24, la fonction d'enregistrement est activée par un détecteur 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 30 août 2018 et de son Règlement d'utilisation, transmis par la Préfecture de la Gruyère par courrier du 17 septembre 2018. En outre, il se réfère au courriel du 9 octobre 2018 du Directeur de l'OCN transmettant les prises de vue de chaque caméra, informations transmises par la Préfecture par courrier du 11 octobre 2018.

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 également des lieux publics, les

immeubles ouverts au public qui sont affectés à l'administration publique (cf. art. 2 al. 2 let. b LVid). Conformément à l'article 1 alinéa 1 LOCN, l'OCN est un établissement de droit public, doté de la personnalité juridique. Au vu des informations fournies par le requérant, les caméras capturent des images du rez-de-chaussée, du SAS d'entrée du hall administratif ainsi que de l'intérieur du hall administratif notamment les 5 guichets du bâtiment de la Succursale de l'OCN de Bulle. 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 dissuader tout comportement violent ou autre mesure de contrainte vis-à-vis du personnel de l'OCN. Le cas échéant, il doit permettre l'identification d'éventuels agresseurs. Il enregistre la clientèle qui se présente à l'espace administratif de la succursale OCN de Bulle/Vuadens ». (cf. art. 1 ch. 3 du Règlement d'utilisation).

Une analyse complète des risques, à la lumière du principe de la proportionnalité, ne figure pas au dossier. En l'état, on peut déduire des éléments à notre disposition 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. Si le dossier ne mentionne pas de cas d'atteinte contre des personnes ou des biens, il est cependant concevable que de telles atteintes puissent survenir à l'encontre tant des collaboratrices et collaborateurs de l'OCN, notamment sur le personnel travaillant aux caisses et celui du secteur des mesures administratives, que des bâtiments et infrastructures.

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, pour prévenir les atteintes aux personnes et aux biens, l'OCN recourt à des guichets partiellement sécurisés ainsi qu'au paiement par cartes. Partant, la vidéosurveillance serait un moyen complémentaire et efficace pour les protéger.

1.3 Quant au but

Il paraît envisageable que le moyen prôné permette de remplir le but poursuivi et de limiter 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 est apte à limiter les atteintes aux biens et aux personnes 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, le système de vidéosurveillance est alimenté par le réseau électrique domestique et relié au moyen d'un réseau informatique fil, de sorte qu'aucun accès via réseau sans fil ou internet n'est prévu. Il ne ressort 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.

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

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

Conformément à ce qui est mentionné à l'article 4 alinéa 1 lettre c LVid ainsi qu'à l'article 8 OVid, tout système de vidéosurveillance devra être 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 la forme de pictogrammes. Des documents à disposition, il ne ressort pas que l'information soit prévue. Ainsi, un chiffre 5 devra être ajouté dans ce sens à l'article 1 du Règlement d'utilisation.

4. Respect du principe de la finalité (art. 4 al. 1 let. c LVid)

La finalité précitée paraît en adéquation avec l'exigence légale.

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

L'organe responsable du système de vidéosurveillance est le directeur, selon l'article 2 alinéa 1 lettre b OVid. Il s'agira d'adapter l'article 2 chiffre 1 du Règlement d'utilisation.

L'article 5 chiffre 3 traite des données sensibles. Pour rappel, toute image est une donnée sensible dans la mesure où elle permet de connaître notamment la race ou le handicap de la personne filmée. Ainsi, il s'agira de modifier dans le sens que « **les images enregistrées sont des données sensibles** au sens de l'article 3 let.c LPrD (notamment les personnes faisant l'objet d'une mesure administrative selon la LCR). Elles sont stockées sur un serveur dédié exclusivement à la vidéosurveillance. Les accès aux données par réseau fil sont limités aux seules personnes citées à l'article 2 chiffre 2 **et protégés selon les modalités définies au chiffre 1 du présent article.** Aucun accès via réseau sans fil ou internet n'est prévu. L'accès physique au serveur est également contrôlé».

Concernant les contrôles techniques de l'installation ainsi que le contrôle des mesures de sécurité, ces derniers doivent être faits par les techniciens internes de l'OCN. En effet, les données traitées sont sensibles, de sorte qu'elles doivent être traitées avec une diligence accrue. Un accès aux données par le fournisseur du système ne peut pas être autorisé, ce qui est en contradiction avec l'article 1 chiffre 2 du Règlement d'utilisation. L'article 5 chiffre 1 dernier paragraphe du Règlement d'utilisation doit également être modifié, à savoir « le fournisseur » doit être supprimé.

Des informations à disposition, il ressort que le serveur dédié exclusivement à l'enregistrement des données de vidéosurveillance du site de Bulle est protégé dans un lieu adéquat au sous-sol du bâtiment et non-accessible à des personnes non-autorisées. Ainsi, l'article 5 devra être complété par un chiffre 4 mentionnant que « le système de stockage des données est protégé dans un lieu adéquat au sein du bâtiment et non-accessible à des personnes non-autorisées ». Il en est également déduit qu'aucun enregistrement n'est hébergé sur un Cloud. En outre, le stockage ainsi que le transfert des données doivent être chiffrés. La clé de chiffrement reste auprès de l'OCN.

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. Informations aux collaboratrices et collaborateurs

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

IV. Conclusion

Dans le cadre de la demande d'installation du système de vidéosurveillance avec enregistrement sis à la **Succursale de l'Office de la circulation et de la navigation**, Rue de Planchy 34, 1628 Vuadens

par

l'Office de la circulation et de la navigation, Route de Tavel 10, 1700 Fribourg,

l'Autorité cantonale de la transparence et de la protection des données émet un préavis **favorable** à la demande d'installation de trois caméras, **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 : pas de visionnement en temps réel mais consultation uniquement en cas d'atteinte avérée, toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons ne doit pas être utilisée.

b. *signalement* : le système de vidéosurveillance devra être 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 la forme d'un pictogramme. Ainsi, un chiffre 5 devra être ajouté dans ce sens à l'article 1 du Règlement d'utilisation.

c. *sécurité des données* : l'organe responsable doit être modifié à l'article 2 chiffre 1 par le directeur ; l'article 5 chiffre 3 du Règlement d'utilisation doit être modifié dans ce sens que « **les images enregistrées sont des données sensibles** au sens de l'article 3 let.c LPrD (notamment les personnes faisant l'objet d'une mesure administrative selon la LCR). Elles sont stockées sur un serveur dédié exclusivement à la vidéosurveillance. Les accès aux données par réseau fil sont limités aux seules personnes citées à l'article 2 chiffre 2 e**t protégés selon les modalités définies au chiffre 1 du présent article**. Aucun accès via réseau sans fil ou internet n'est prévu. L'accès physique au serveur est également contrôlé » ; les contrôles techniques de l'installation ainsi que le contrôle des mesures de sécurité doivent être effectués par les techniciens internes de l'OCN ; tout mandataire ou fournisseur ne peut avoir accès aux données enregistrées, l'article 1 chiffre 2 du Règlement d'utilisation doit être modifié en ce sens ainsi que « le fournisseur du système » doit être supprimé de l'article 5 chiffre 1 dernier paragraphe ; l'article 5 devra être complété par un chiffre 4 mentionnant que « le système de stockage des données est protégé dans un lieu adéquat au sein du bâtiment et non-accessible à des personnes non-autorisées » ; les enregistrements ne sont pas stockés dans un Cloud ; le stockage et le transfert des données sont chiffrés et les clés de chiffrement sont en main de l'OCN.

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

V. Remarques

> 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 30a al. 1 let. c LPrD est réservé.

> Le présent préavis sera publié.

Alice Reichmuth Pfammatter
Préposée cantonale à la protection des données

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