



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. : dossier 8066 RPA/GG

PRÉAVIS du 23 octobre 2013

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

Demande d'autorisation d'installation de vidéosurveillance

Banque Raiffeisen Vuadens/Sâles/St-Martin, route Principale 174, 1628 Vuadens

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),

L'Autorité cantonale de la transparence et de la protection des données formule le présent préavis concernant la requête de la Banque Raiffeisen Vuadens/Sâles/St-Martin, visant à l'installation d'un système de vidéosurveillance avec enregistrement, comprenant quatre caméras de marque Siemens, sans zoom, fonctionnant 24h/24. Le système de vidéosurveillance fait l'objet de ce préavis pour autant que le champ de vision de ses caméras couvrent tout ou partie de lieux publics (art. 2 al. 1 LVid). Au vu des informations fournies par le requérant, une caméra (à l'intérieur du bancomat) capture des images en gros plan de toute personne effectuant un retrait et les trois autres (au plafond), filment avec un champ de vision plus large et capturent des images de toute activité au bancomat et dans un proche périmètre.

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 13 novembre 2012, des compléments d'informations requis par courrier du 21 mars 2013 et de son Règlement d'utilisation (Annexe 1), transmis par la Préfecture de la Gruyère par courrier du 26 septembre 2013.

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 filmer toute personne entrant dans la zone 24 heures et qui veut utiliser le bancomat. Ces enregistrements permettront d'observer une scène en cas d'agression d'un utilisateur et d'en reconnaître l'auteur. De même les personnes apportant des modifications non autorisées sur l'appareil (skimming par exemple) pourront être identifiées » (cf. art. 1 ch. 3 du Règlement d'utilisation).

Une analyse 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'atteintes contre des personnes ou des biens, il est cependant concevable que de telles atteintes puissent survenir à l'encontre des utilisateurs des bancomats, lors d'un retrait d'argent en espèces.

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 protéger les utilisateurs du bancomat Raiffeisen sis à Vuadens, il semble que la vidéosurveillance soit un moyen efficace pour y parvenir. Le nombre de caméras (4) paraît important. La Banque Raiffeisen Vuadens/Sâles/St-Martin doit être rendue attentive que le champ de vision des caméras ne doit pas couvrir des espaces privés. Le cas échéant, des masques de confidentialité (*privacy mask*) devront être mis en place afin de limiter l'atteinte aux droits fondamentaux et ainsi être en conformité avec le principe de la proportionnalité.

1.3 Quant au but

Comme mentionné au point II. 1, le but du présent système est « de filmer toute personne entrant dans la zone 24 heures et qui veut utiliser le bancomat. Ces enregistrements permettront d'observer une scène en cas d'agression d'un utilisateur et d'en reconnaître l'auteur. De même les personnes apportant des modifications non autorisées sur l'appareil (skimming par exemple) pourront être identifiées ». Dès lors, il paraît envisageable que les moyens prônés permettent de remplir le but poursuivi et de limiter les risques cités plus haut.

III. Conditions

1. Exigence de la base légale

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

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. En l'état, il apparaît que le choix est dicté par le fait qu'aucun autre système ne permette de remplir le but visé, tout en étant économiquement supportable (p. ex. substitution de la caméra par un vigile ou un système d'alarme).

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

Conformément à ce qui est mentionné à l'art. 4 al. 1 let. c LVID ainsi qu'à l'art. 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 ressort qu'une information est prévue. Toutefois, conformément à l'art. 8 OVID, le panneau doit informer sans équivoque les personnes se trouvant dans la zone surveillée de l'existence de l'installation et *mentionner le responsable du système*.

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

Le principe de la finalité au sens de l'art. 5 LPrD est respecté dans la mesure où les données sont traitées conformément à l'art. 3 al. 1 LVID, à savoir de prévenir *les atteintes aux personnes et aux biens et de contribuer à la poursuite et à la répression des infractions*. Il apparaît, selon les informations à notre disposition, que le but visé par le requérant, est *de filmer toute personne entrant dans la zone 24 heures et qui veut utiliser le bancomat. Ces enregistrements permettront d'observer une scène en cas d'agression d'un utilisateur et d'en reconnaître l'auteur. De même les personnes apportant des modifications non autorisées sur l'appareil (skimming par exemple) pourront être identifiées*. Cette finalité paraît en adéquation avec l'exigence légale.

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

L'art. 5 ch. 3 du Règlement d'utilisation dispose que « lorsque des données sont identifiées comme étant sensibles au sens de l'art. 3 let. c LPrD, leur accès est protégé de la façon suivante : les titulaires d'autorisation personnelle reçoivent alors un mot de passe qu'ils modifient régulièrement ». Au terme de l'art. 3 let. c LPrD, sont des données sensibles, « les données personnelles sur : les opinions ou activités religieuses, philosophiques, politiques ou syndicales (ch. 1) ; la santé, la sphère intime ou l'appartenance à une race (ch. 2) ; des mesures d'aide sociale (ch. 3) ; des sanctions pénales ou administratives et les procédures y relatives (ch. 4) ». Or, notre Autorité a toujours considéré que le contexte pouvait rendre des données sensibles. C'est le cas de prises de vue qui donneraient des informations par ex. sur la race, la sphère intime (accompagnants) et la santé (handicapés). Selon les informations à notre disposition, la sécurité des données, au cas où il devait s'agir de données sensibles, semble garantie avec les mesures prévues (accès protégé par un mot de passe).

Par ailleurs, les données ne doivent être accessibles que par les personnes autorisées, comme cela est mentionné à l'art. 2 ch. 2 du Règlement d'utilisation. Finalement, le système doit être protégé dans un lieu adéquat et non-accessible à des personnes non-autorisées.

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 doivent être conservées pendant *trente jours*, sauf en cas d'atteintes aux personnes ou aux biens auquel cas le délai peut être porté à cent jours (art. 4 ch. 3 du Règlement d'utilisation), ce qui est conforme avec la législation en vigueur.

IV. Conclusion

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

préavis favorable à la demande d'autorisation d'un système de vidéosurveillance

par

la Banque Raiffeisen Vuadens/Sâles/St-Martin, route Principale 174, 1628 Vuadens, aux conditions suivantes :

- a. *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 de pictogramme.
- b. *sécurité des données* : le système doit être protégé dans un lieu adéquat et non-accessible à des personnes non-autorisées.

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 d'autres organes publics ou à des personnes privées.
- > Le requérant est rendu attentif que s'il filme ses employés, il est soumis aux règles de la Loi fédérale du 19 juin 1992 sur la protection des données (RS 235.1; LPD). Nous renvoyons le requérant à la prise de position du préposé fédéral sur le sujet : <http://www.edoeb.admin.ch/themen/00794/00800/00911/index.html?lang=fr>.
- > 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'art. 30a al. 1 let. c LPrD est réservé.


Alice Reichmuth Pfammatter
Préposée cantonale à la protection des données

Annexes

- formulaire de demande d'autorisation d'installer un système de vidéosurveillance
- règlement d'utilisation