COMMUNE DE **BELFAUX**

Règlement d'utilisation des installations de vidéosurveillance avec enregistrement

Le Conseil communal de Belfaux,

vu :

- la loi du 7 décembre 2010 sur la vidéosurveillance (LVid)
- l'article 60 al. 3 let. m de la loi sur la vidéosurveillance (LVid)
- l'ordonnance du 23 août 2011 sur la vidéosurveillance (OVid),
- la loi du 25 novembre 1994 sur la protection des données(LPrd),
- le règlement du 29 juin 199 sur la sécurité des données personnelles (RSD),
- le code du 23 mai 1991 de procédure et de juridiction administrative (CPJA)

adopte le règlement d'utilisation suivant :

Art. 1 Objet

1. Le présent règlement s'applique aux systèmes de vidéosurveillance avec enregistrement placés sur le territoire de la commune de Belfaux.

2. Les systèmes de vidéosurveillance, objet du présent règlement, sont composés de caméras du type mini dôme HDBW2431RP-ZS-S 4MP, de serveur de type NVR 32 voies – sorties 4K – Intel Processor – Max 32 IP/ Caméra Inputs accessibles par réseau informatique sécurisé (IP fixe) et d'un logiciel de traitement des données (Logiciel Dahua Smart PPS).

3. Ces systèmes de vidéosurveillance ont pour but la prévention des actes de vandalisme et l'identification des personnes ayant causé des dégâts au patrimoine communal.

4. Le système de vidéosurveillance fonctionnera du lundi au vendredi de 17h00 à 07h00 et 24h/24 le week-end, les jours fériés et pendant les vacances scolaires.

5. Le Conseil communal publie sur son site internet la liste des lieux placés sous vidéosurveillance ainsi qu'un plan de situation indiquant les endroits où sont placées les caméras. En outre, 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.

Art. 2 Organes et personnes autorisées

1. Le Conseil communal est l'organe responsable du système de vidéosurveillance.

2. Les personnes autorisées à consulter les données enregistrées par le système de vidéosurveillance sont :
   - Accès aux enregistrements : le/la responsable d'établissement, le/la concierge
   - Autorisation d'extraction : le/la syndic/que et le/la secrétaire communal/e
   - Accès aux serveurs : le/la responsable d'établissement et le/la concierge

3. Pour tout accès direct aux images, les utilisateurs doivent changer régulièrement de mot de passe et une double authentification est nécessaire.

4. Ces personnes sont soumises au secret de fonction, respectivement aux règles de confidentialité.

Art. 3 Données mises à disposition

1. Les données consultables par les personnes mentionnées à l'art. 2 ci-dessus sont les images enregistrées par l'installation de vidéosurveillance.

2. Un devoir de diligence accru s'applique (cf. art. 8 LPrD) lorsque des images ainsi obtenues contiennent des données dites sensibles au sens de l'art. 3 let. c LPrD.

Art. 4 Traitement des données

1. Les données enregistrées ne devront être utilisées que dans le cadre du but défini à l'article 1 al. 3 ci-dessus.

2. Les images enregistrées ne sont pas visionnées en temps réel.

3. Les titulaires d'autorisation personnelle consultent les images enregistrées qu'en cas de nécessité, à savoir en cas d'atteinte avérée.

4. Les personnes autorisées à consulter les données sont susceptibles d'être interrogées en tout temps, y compris au-delà de l'exercice de leurs fonctions, sur les données qu'elles auront visionnées ou sur les agissements en relation avec ces données.

5. Les données enregistrées sont automatiquement détruites après 7 jours. En cas d'atteinte avérée aux personnes ou aux biens, les données enregistrées sont extraites sur un support informatique sécurisé et sont détruites après 100 jours au maximum. Un protocole de destruction est conservé.

6. Des copies ou impressions peuvent être effectuées mais doivent être détruites dans les mêmes délais que les originaux. Un protocole de copie est conservé.

7. La commercialisation d'éventuelles impressions et reproductions est interdite.

8. Toute communication de données est interdite en dehors du cadre légal (art. 4 al. 1 let. e LViD).

9. Toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons, voire permettant la reconnaissance faciale, n'est pas autorisée.

Art. 5 Mesures de sécurité

1. Les données informatiques sont protégées par l'organe responsable du fichier de la façon suivante :

- une autorisation personnelle d'accès est délivrée par le Conseil communal aux personnes autorisées pour lesquelles un accès est nécessaire en raison de leur fonction (cf. art. 2 ch. 2) ;
- les titulaires d'autorisation personnelle consultent les images enregistrées qu'en cas de nécessité, à savoir qu'en cas d'atteinte avérée (cf. art. 2 ch. 2) ;
- les personnes autorisées bénéficient d'un accès (mot de passe) et modifient régulièrement leur mot de passe (cf. art. 2 ch. 2) ;
- une double authentification est recommandée.

2. Toute activité effectuée sur le système ou sur des applications informatiques est automatiquement enregistrée et répertoriée à des fins de contrôle et/ou de reconstitution. Un journal d'accès est imprimé chaque mois. Il est conservé une année au moins en sécurité sous clé, dans les locaux de l'administration communale. Le journal est transmis mensuellement à l'organe de contrôle interne défini à l'art. 6 let. a.

3. Le système de stockage et d'hébergement des données (et/ou le back-up) doivent être protégés in situ, dans un lieu adéquat, fermé à clé, sans accès à distance et non accessible aux personnes non autorisées (cf. art. 2 ch. 2).

4. Les images enregistrées et celles extraites doivent être stockées sur un support physique indépendant, sans accès à distance possible (réseaux sans fils ou internet) et, est remis, le cas échéant, au procureur ou au juge en charge de la procédure. Seules les personnes autorisées ont accès au serveur local (cf. art. 2 ch.2).

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

Art. 6 Mesures de contrôle

a. Contrôles internes

1. Des contrôles techniques des installations de vidéosurveillance ainsi que le contrôle du respect des mesures de sécurité sont effectués par les personnes mentionnées à l'art. 2 alinéa 2.

2. Il convient notamment de vérifier l'orientation des caméras, le respect de leur programmation (horaire) et leur signalisation.

3. Chaque contrôle fait l'objet d'un protocole dûment signé par le responsable de l'installation.

b. Contrôle général

1. Le ou la Préfet/e exerce un contrôle général sur les installations de vidéosurveillance

2. Les contrôles du ou de la préposé/e cantonal/e à la protection des données sont en outre réservés.

Art. 7 Droit d'accès

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).

Art. 8 Entrée en vigueur

Le présent règlement entre en vigueur dès son adoption par le Conseil communal.

Adopté par le Conseil communal de Belfaux, le 10.05.2022

AU NOM DU CONSEIL COMMUNAL

Muriel Frésard
Syndique

CONSEIL COMMUNAL - 1782 BELFAUX

Laurent Wolfer
Secrétaire communal

Le présent règlement a été approuvé par le Lieutenant de Préfet de la Sarine le 21 juin 2022.

ETAT DE FRIBOURG - STAAT FREIBURG

Patrick NICOLET
Lieutenant de Préfet