|  |
| --- |
| Règlement d’utilisation de l’installation de vidéosurveillance avec enregistrement |

(*Nom de l’organe, de la collectivité ou de la personne privée*),

vu

la loi du 7 décembre 2010 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 1999 sur la sécurité des données personnelles (RSD)

adopte le règlement d’utilisation suivant :

**Art. 1 Objet**

1. Le présent règlement s’applique au système de vidéosurveillance avec enregistrement placé (*description du lieu et de l’adresse*).

2. Le système de vidéosurveillance objet du présent règlement est composé de *(description précise du système - marque et type de caméra, alimentation, communication par WiFi ou par câbles, possibilités techniques - zoom, enregistrement, etc.)*

3. Ce système de vidéosurveillance a pour but … . et permettra d’observer ….

4. Il fonctionnera *(horaires)*.

5. (*éventuellement autres points*).

**Art. 2 Organes et personnes autorisées**

1. Le (*nom de l’organe*) est l’organe responsable du système de vidéosurveillance.

2. Les personnes autorisées à consulter les données enregistrées par le système de vidéosurveillance sont les suivantes :

- (*nom, prénom, fonction*)

- (*nom, prénom, fonction*)

Ces personnes sont soumises à l’obligation du respect du secret de fonction, respectivement de confidentialité.

3. (*éventuellement autres points*).

**Art. 3 Données mises à disposition**

1. Les données consultables par les personnes susmentionnées (art. 2 ci-dessus) sont les images récoltées et enregistrées par l’installation de vidéosurveillance.
2. Il se peut que les images ainsi obtenues contiennent des données dites sensibles au sens de l’art. 3 let. c LPrD ; dès lors, un devoir de diligence accru s’applique (cf. art. 8 LPrD).
3. (*éventuellement autres points*).

**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 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 leurs agissements en relation avec ces données.
3. Les données enregistrées doivent être détruites après 30 jours ou, en cas d’atteinte aux personnes ou aux biens, après 100 jours au maximum.

Un protocole de destruction est conservé.

1. Des copies ou impressions peuvent être effectuées mais doivent être détruites dans les mêmes délais que les originaux.

Un protocole de copie est conservé.

1. La commercialisation d’éventuelles impressions et reproductions est interdite.
2. Toute communication de données est interdite, en dehors du cadre légal (art. 4 al. 1 let. e LVid).
3. (*éventuellement autres points*).

**Art. 5 Mesures de sécurité**

1. Les données informatiques sont protégées par l’organe responsable du fichier de la façon suivante : (*énumérer les mesures*)

- une autorisation personnelle d’accès (mot de passe) est délivrée aux collaborateurs pour lesquels un accès est nécessaire en raison de leur fonction ;

- les titulaires d’autorisation personnelle reçoivent alors un mot de passe qu’ils modifient régulièrement ;

- … .

1. Toute activité effectuée sur un système ou sur une application informatique sera automatiquement enregistrée et répertoriée à des fins de contrôle ou de reconstitution.
2. 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 : (*indiquer la mesure appropriée*).
3. Les images enregistrées doivent être stockées sur un support physique indépendant, sans accès à distance possible (réseaux sans fils ou internet).
4. (*éventuellement autres points*).

**Art.** **6 Mesures de contrôle**

1. **Contrôles internes**
2. Des contrôles techniques de l’installation ainsi que le contrôle du respect des mesures de sécurité sont effectués par (*indiquer l’organe de contrôle*) tous les (indiquer la fréquence).
3. Il convient notamment de vérifier l’orientation de la caméra, le respect de sa programmation (horaire) et sa signalisation.
4. Chaque contrôle fera l’objet d’un protocole dûment signé par le responsable de l’installation.
5. (*éventuellement autres points*).
6. **Contrôle général**
7. Le préfet exerce un contrôle général sur les installations de vidéosurveillance.
8. Les contrôles du ou de la préposé/e cantonal/e à la protection des données sont en outre réservés.

**Art. 7 Entrée en vigueur**

Le présent règlement entre en vigueur (soit immédiatement lors de la mise en place de l’installation de vidéosurveillance, savoir le …., soit, si l’installation est pré-existante : le (*date*).

Le présent règlement a été adopté par……………….. le……………………

Signatures

Le présent règlement a été approuvé par le Préfet de ………….. le………………

Signature