|  |
| --- |
| Règlement d’utilisation d’un système 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 – nombre de caméra, marque et type de caméra, alimentation, communication par WiFi ou par câbles, possibilités techniques - zoom, enregistrement, etc.)* (cf. Annexe*)*
3. Ce système de vidéosurveillance a pour but … . et permettra d’observer ….
4. Il fonctionnera *(horaires : heure/jour/sur détection de mouvement)*.
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 (enregistrements) par le système de vidéosurveillance sont les suivantes (*deux à trois personnes maximum) :*

 - (*nom, fonction*)

 - (*nom, fonction*)

1. Les personnes autorisées (ex. personnel du guichet/de la réception) à visionner en temps réel les images sont les suivantes :

- (nom, fonction)

- (nom, fonction)

1. Les personnes susmentionnées sont soumises à l’obligation du respect du secret de fonction, respectivement de confidentialité.
2. (*éventuellement autres points*).

**Art. 3 Données mises à disposition**

1. Les données consultables par les personnes susmentionnées (art. 2 ch. 2 ci-dessus) sont les images récoltées et enregistrées par l’installation de vidéosurveillance.
2. Les données visionnées en direct par les personnes susmentionnées (art. 2 ch. 3 ci-dessus) sont les images des caméras suivantes *(numérotation selon annexe)* :
3. Il se peut que les images obtenues ainsi contiennent des données dites sensibles au sens de l’art. 3 let. c LPrD, de sorte qu’un devoir de diligence accru s’applique (cf. art. 8 LPrD).
4. (*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 images enregistrées (*sont ou ne sont pas*) visionnées en temps réel, pendant les horaires suivants : …….. (cf. Annexe).
3. Sous réserve de la vision en temps réel, 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 leurs agissements en relation avec ces données.
5. Les données enregistrées sont automatiquement détruites après 30 jours. En cas d'atteinte avérée aux personnes ou aux biens, les données enregistrées sont extraites sur un support informatique et sont détruites après 100 jours au maximum sous réserve de leur transmission à une autorité judiciaire ou à la Police cantonale à des fins d’enquête. 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 est interdite. L’organe responsable n’est pas autorisé à utiliser de fonctionnalité permettant la reconnaissance faciale, l’analyse des données ou toute autre fonctionnalité relevant de l’intelligence artificielle.
10. (*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 personnes autorisées (cf. art. 2) pour lesquels un accès un nécessaire en raison de leur fonction ;
	* les titulaires d’autorisation personnelle reçoivent alors un mot de passe qu’ils modifient régulièrement ;
	* une double authentification est recommandée ;
	* *(éventuellement autres points)*
2. Toute activité effectuée sur le système ou sur une des applications informatiques sera automatiquement enregistrée et répertoriée à des fins de contrôle et/ou de reconstitution.
3. Le système de stockage et d’hébergement des données (et/ou la *back-up*) doivent être protégés dans un lieu adéquat en Suisse, fermé à clé et non-accessible aux personnes non-autorisées.
4. Les images enregistrées et celles extraites doivent être stockées sur un support physique indépendant, sans accès à distance possible. Seules les personnes autorisées ont accès au serveur local (cf. art. 2 ch. 2).
5. Le transfert ainsi que le stockage des données doivent être chiffrés.
6. L’organe responsable s’assure des mesures techniques et organisationnelles concernant l’accès des personnes autorisées aux enregistrements et aux images en temps réel, notamment s’agissant des appareils utilisés.
7. (*éventuellement autres points*).

**Art.** **6 Droit d’accès**

1. Toute personne peut demander au responsable du système l’accès à ses propres données.
2. Le responsable du système répond à la demande tout en respectant les droits de la personnalité des autres personnes concernées (p. ex. en les floutant).

**Art. 7 Signalement**

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. 8 Responsabilité**

1. L’organe responsable demeure responsable de la protection des données envers d’éventuels mandataires et/ou sous-traitants. Il leur donne, à ce sujet, les instructions nécessaires et veille à ce que les données ne soient utilisées et/ou communiquées que conformément et pour l’exécution du contrat.
2. Le contrat est annexé au Règlement d’utilisation. Il contient les mesures organisationnelles et techniques exigées par l’organe responsableainsi qu’une clause de confidentialité.
3. Les collaboratrices et collaborateurs du contractant signent une clause de confidentialité. Celle-ci est annexée au Règlement d’utilisation.

**Art. 9 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*). Ces contrôles ont lieu sur le site en présence d'une personne autorisée (cf. art. 2 ch. 2).
3. Il convient notamment de vérifier l’orientation de chaque caméra, le respect de leur programmation (horaire) et leur 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. 10 Entrée en vigueur**

Le présent règlement entre en vigueur au moment de son approbation préfectorale.

Adopté par (*Nom de l’organe, de la collectivité ou de la personne privée*), le…………………..

*Formule-s de signature à adapter selon le·la requérant·e*

Approuvé par

*A compléter sur instruction de la Préfecture concernée dans le cadre de la procédure*

**Annexe :**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No de la caméra** | **Description du système** | **Emplacement de la caméra** | **Marque** | **Type de transmission** (Wifi ou câble) | **Possibilités techniques** (zoom, etc.) | **Enregistrement** (oui ou non) | **Horaires enregistrement** | **Vision en****temps réel**(oui ou non, par qui) | **Horaire vision en temps réel** | **Particularité-s**(ex. cache ou bloque noir pour les habitations en arrière-fond, etc.  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |