

VILLARS-SUR-GLÂNE



**REGLEMENT D'UTILISATION
DES INSTALLATIONS DE
VIDEOSURVEILLANCE
AVEC ENREGISTREMENT**

REGLEMENT D'UTILISATION DES INSTALLATIONS DE VIDEOSURVEILLANCE AVEC ENREGISTREMENT

Le Conseil communal de Villars-sur-Glâne

VU

- la loi du 7 décembre 2010 sur la vidéosurveillance (LVid);
- l'ordonnance du 23 août 2011 sur la vidéosurveillance (OVid) ;
- la loi du 12 octobre 2023 sur la protection des données (LPrD) ;
- le règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD) ;
- l'article 60 al. 3 let. m de la loi du 25 septembre 1980 sur les communes (LCo) ;

adopte le règlement d'utilisation suivant :

Art. 1 Objet

¹ Le présent règlement s'applique aux systèmes de vidéosurveillance avec enregistrement placés aux abords **des écoles suivantes** :

- école primaire des Rochettes, Route du Soleil 10 (4 caméras);
- école primaire de Villars-Vert, Route de Villars-Vert 48-50 (4 caméras) ;
- école primaire de Cormanon, Route de la Berra 2 (4 caméras) ;
- école primaire du Platy, Allée du Château 11-13-15 (3 caméras) ;
- centre scolaire de Villars-Vert, Route de Villars-Vert 42-44-46 (6 caméras) ;

et des bâtiments publics suivants :

- centre sportif du Platy, Route du Centre-Sportif 1 (2 caméras) ;
- buvette du FC Villars, Route du Centre-Sportif 3 (1 caméra) ;
- réservoir de Belle-Croix, Bois de Belle-Croix 3 (2 caméras).

² Le système de vidéosurveillance multi-site, objet du présent règlement est composé de caméras de type Dome 6 MP (DS-2CD2166G2-I et DS-2CD2766G2-IZS) avec enregistreurs NVR 8xIP@12 MP (avec disques Western Digital HDD) sur réseau informatique sécurisé.

³ Ces systèmes de vidéosurveillance ont pour but la protection des personnes et la prévention des actes de vandalisme et d'atteinte au patrimoine communal, l'identification des personnes ayant causé des dégâts et la répression des infractions commises.

⁴ Les caméras enregistreront au moyen d'un système de détection de présence tous les jours, 24 heures sur 24. Les caméras situées sur les sites scolaires n'enregistreront pas entre 7h00 et 18h00 durant les jours de classe.

Art. 2 Organes et personnes autorisés

¹ Le Conseil communal est l'organe responsable du système de vidéosurveillance. Il délègue la gestion du système à l'Association de communes pour l'exploitation d'un corps de police intercommunale (ACoPol).

² Les personnes autorisées à consulter les données enregistrées par les systèmes de vidéosurveillance sont les agents assermentés de l'ACoPol. Trois agents sont désignés par le ou la chef-fe du corps de police intercommunale.

³ Ces personnes sont soumises à l'obligation du respect du secret de fonction, respectivement de confidentialité. L'identité de ces personnes est consignée par l'organe responsable dans un document qui est actualisé si elles sont remplacées.

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 les installations de vidéosurveillance.

² Il se peut que les images ainsi obtenues contiennent des données dites sensibles au sens de l'art. 4 al. 1 let. c LPrD, dès lors, un devoir de diligence accru s'applique (cf. art. 11 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 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.

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 (mot de passe) est délivrée aux personnes autorisées (cf. art. 2) 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.

² Toute activité effectuée sur un système ou sur une application informatique 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, notamment s'agissant des appareils utilisés.

Art. 6 Droit d'accès

¹ Toute personne peut demander à l'organe responsable l'accès à ses propres données.

² L'organe responsable 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

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.

Art. 9 Mesures de contrôle

a. Contrôles internes

¹ Des contrôles techniques de l'installation ainsi que le contrôle du respect des mesures de sécurité sont effectués par les agents assermentés de l'ACoPol toutes les semaines.

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

³ Chaque contrôle fera l'objet d'un protocole dûment signé.

b. Contrôle général

¹ Le ou la Préfet-ète 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. 10 Entrée en vigueur

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

Ainsi adopté par le Conseil communal, le 17 mars 2025

AU NOM DU CONSEIL COMMUNAL

Le Secrétaire


Emmanuel Roulin



Le Syndic


Bruno Marmier

Approuvé par la Préfète de la Sarine

le 14.05.2025

Lise-Marie Graden



