



**Règlement d'utilisation
d'un système de vidéosurveillance avec enregistrement**

La Commune de Billens-Hennens,

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 installé route de Prévonloup 25 (déchetterie) à Billens.
2. Le système de vidéosurveillance objet du présent règlement est composé de caméras IP Synology 8C500 et TC500K (cf. Annexe).
3. Ce système de vidéosurveillance a pour but de prévenir les atteintes aux personnes et aux biens de la déchetterie et de contribuer à la répression des infractions.
4. Il fonctionnera en dehors des heures d'ouverture de la déchetterie.
5. Les vues sur le terrain de football et sur la route cantonale seront masquées par le logiciel d'enregistrement.

Art. 2 Organes et personnes autorisées

1. Le Conseil communal de Billens-Hennens 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*) :
 - Le Syndic ;
 - Le Vice-syndic ;
 - Le Conseiller communal en charge de la Police.
3. Les personnes susmentionnées sont soumises à l'obligation du respect du secret de fonction, respectivement de confidentialité.

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. 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).

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 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 et sont détruites après 100 jours au maximum. Un protocole de destruction est conservé.
4. Des copies ou impressions peuvent être effectuées mais doivent être détruites dans les mêmes délais que les originaux. Un protocole de copie est conservé.
5. La commercialisation d'éventuelles impressions et reproductions est interdite.
6. Toute communication de données est interdite, en dehors du cadre légal (art. 4 al. 1 let. e LVID).
7. Toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons est interdite. L'organe responsable n'est pas autorisé à utiliser des fonctionnalités 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 le système ou sur une des applications informatiques sera automatiquement enregistrée et répertoriée à des fins de contrôle et/ou de reconstitution.
3. Lorsqu'un cas d'atteinte est avéré, seules les personnes autorisées sont habilitées à extraire et exporter la séquence de données sur un support de stockage externe pour transmissions aux autorités compétentes lors d'un dépôt de plainte.
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. L'organe responsable s'assure des mesures techniques et organisationnelles concernant l'accès des personnes autorisées aux enregistrements, notamment s'agissant des appareils utilisés.
6. Un pictogramme indiquera clairement aux personnes présentes que les lieux sont sous surveillance vidéo.

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 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 chaque année. Ces contrôles ont lieu sur le site en présence d'une personne autorisée (cf. art. 2 ch. 2).
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 par le responsable de l'installation.

b. Contrôle général

1. Le préfet 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. 8 Entrée en vigueur

Le présent règlement entre en vigueur dès son approbation.

Le présent règlement a été adopté par le Conseil communal, le 16 juin 2025.

AU NOM DU CONSEIL COMMUNAL

Le Syndic

Florian Dubail

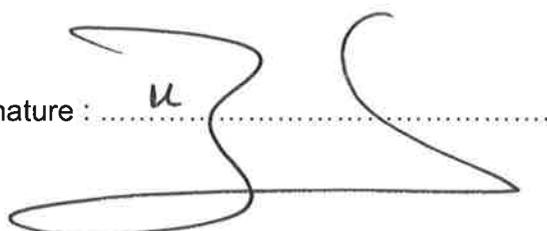


La Secrétaire

Alexandra Lovati

Le présent règlement a été approuvé par le Préfet de la Glâne, le :

24 juin 2025

Signature : 

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.
1	Benne	Angle nord-ouest déchetterie	Synology	Câble		oui	Heures de fermeture	non		Terrain de football caché
2	Accès principal déchetterie	Angle nord-ouest déchetterie	Synology	Câble		oui	Heures de fermeture	non		Route cantonale caché

