

# Préavis municipal n° 17-2018 au Conseil communal de Cugy VD

## Révision partielle du Règlement communal relatif à l'utilisation de caméras de vidéosurveillance dissuasive

Monsieur le Président,  
Mesdames et Messieurs les Conseillères et Conseillers,

Nous avons l'honneur de soumettre à votre approbation le préavis municipal n° 17-2018 relatif à la révision partielle du Règlement communal relatif à l'utilisation de caméras de vidéosurveillance dissuasive.

### 1. Objet du préavis

Le présent préavis a pour objectif de vous soumettre l'adoption de la révision partielle du Règlement communal relatif à l'utilisation de caméras de vidéosurveillance dissuasive de 2013 en vue de l'adapter à une récente révision de la loi vaudoise du 11 septembre 2007 sur la protection des données personnelles (LPrD<sup>1</sup>), entrée en vigueur le 1<sup>er</sup> octobre 2018<sup>2</sup>, qui permet, en particulier, d'étendre la durée maximale de conservation des images.

Pour les communes dotées d'un règlement communal prévoyant une durée de conservation maximale de 96 heures, comme nous le connaissons à Cugy, il convient de modifier le règlement en question avant de pouvoir bénéficier de cette extension du délai de préservation des images vidéo.

### 2. Contexte

Le Conseil communal a adopté le 21 mars 2013 le Règlement communal de 2013 relatif à l'utilisation de caméras de vidéosurveillance dissuasive<sup>3</sup>. Celui-ci est entré en vigueur le 1<sup>er</sup> mai 2013 après approbation de la Cheffe du Département de l'intérieur.

Ce texte normatif répondait au constat d'une recrudescence d'actes d'incivilités et de déprédations commises à l'encontre des bâtiments communaux et de celui de l'ASICE. Le dispositif de vidéosurveillance visait ainsi à protéger, de manière dissuasive, les bâtiments publics les plus exposés contre la perpétration d'actes malveillants et à contenir les frais de réparation et/ou de nettoyage à la charge de la Commune à la suite de l'accomplissement de ces délits.

Depuis l'installation du système de vidéosurveillance en 2015, ce dispositif a été mobilisé à quatre reprises. Dans trois cas, des images ont pu, après dépôt de plainte, être remises à la Police cantonale en vue de l'identification des délinquants. A cet usage répressif, s'ajoute l'aspect dissuasif, impossible cependant à mesurer, mais qui a vraisemblablement permis d'éviter la survenance d'autres cas délictueux au vu du risque d'être identifié.

Après un peu plus de trois ans d'exploitation, ce dispositif fonctionne à satisfaction de la Municipalité. Cependant, force est de constater que la limitation actuelle de la durée maximale de

<sup>1</sup> Loi sur la protection des données personnelles du 11 septembre 2007 (LPrD ; RSV 172.65).

<sup>2</sup> Loi modifiant celle du 11 septembre 2007 sur la protection des données personnelles du 5 juin 2018, publié dans la FAO du 19 juin 2018 ; Arrêté de mise en vigueur du 5 septembre 2018, publié dans la FAO du 11 septembre 2018.

<sup>3</sup> Préavis municipal n° 19-2013 Règlement communal relatif à l'utilisation de caméras de vidéosurveillance dissuasive.

conservation des images à 96 heures a compliqué dans certains cas la gestion opérationnelle du système. En effet, les délits sont généralement annoncés à l'Administration communale 24 à 48 heures après leur survenance, voire plus, ce qui laisse très peu de temps pour préserver les images nécessaires, en particulier lors des week-ends ou périodes de vacances. Cette limitation accentue le risque de perdre d'importantes preuves pour la résolution des enquêtes de Police et limite ainsi l'efficacité potentielle de ce système de vidéosurveillance.

La nouvelle entrée en vigueur le 1<sup>er</sup> octobre 2018 modifie notamment le régime existant en matière de vidéosurveillance dissuasive.

Parmi les évolutions contenues dans ce texte figure le transfert de compétence aux Préfectures pour l'approbation de ces dispositifs (art. 22a nouveau LPrD) – processus qui dépendait jusqu'alors du Bureau de la Préposée à la protection des données et à l'information –, ainsi que la possibilité, hors de toute procédure pénale, d'étendre la durée maximale de conservation des images, qui passe de 96 heures à 7 jours ou, en cas d'atteinte aux personnes ou aux biens, à 100 jours (art. 23a nouveau LPrD).

L'augmentation de cette durée de conservation décidée par le législateur, tout en pérennisant les strictes dispositions en matière de protection des données, offre une flexibilité bienvenue dans l'exploitation d'un dispositif de vidéosurveillance tel que le nôtre.

Selon les dispositions transitoires, notre commune dispose d'un délai de cinq ans pour se conformer aux exigences de la nouvelle LPrD (art. 42 nouveau LPrD).

### 3. Modifications proposées

En vue d'adapter notre Règlement communal de 2013 relatif à l'utilisation de caméras de vidéosurveillance dissuasive à la dernière mouture de la Loi sur la protection des données personnelles (LPrD), la Municipalité sollicite une modification des art 1, 4, 5, et 9, toutes basées sur le règlement-type du 2 août 2018 :

Règlement actuel	Modification proposée
<p><b>Article premier – Principe</b></p> <p>Un système de vidéosurveillance dissuasive peut, après avoir obtenu l'autorisation <del>du Préposé à la protection des données et à l'information</del>, être installé sur le domaine public ou le patrimoine administratif communal dans le but d'éviter la perpétration d'infractions contre des personnes et des biens et d'apporter des moyens de preuve en cas de telles infractions. Il doit constituer, si possible en complément d'autres mesures, le moyen le plus adéquat pour atteindre le but fixé.</p>	<p><b>Article premier – Principe</b></p> <p>Un système de vidéosurveillance dissuasive peut, après avoir obtenu l'autorisation <u>de l'autorité compétente</u>, être installé sur le domaine public ou le patrimoine administratif communal dans le but d'éviter la perpétration d'infractions contre des personnes et des biens et d'apporter des moyens de preuve en cas de telles infractions. Il doit constituer, si possible en complément d'autres mesures, le moyen le plus adéquat pour atteindre le but fixé.</p>

Cette modification permet de retirer la mention du Préposé à la protection des données et à l'information qui n'est plus l'autorité de délivrance des autorisations en matière de vidéosurveillance. Cette compétence est dorénavant déléguée aux Préfectures.

<p><b>Art. 4 Sécurité des données</b></p> <p>Des mesures de sécurité appropriées sont prises afin d'éviter tout traitement illicite des données, notamment en limitant l'accès aux données enregistrées et aux locaux qui les contiennent.</p> <p><del>Le contrôle des accès aux images sera garanti.</del></p>	<p><b>Art. 4 Sécurité des données</b></p> <p>Des mesures de sécurité appropriées sont prises afin d'éviter tout traitement illicite des données, notamment en limitant l'accès aux données enregistrées et aux locaux qui les contiennent.</p> <p><u>Un système de journalisation automatique permet de contrôler les accès aux images.</u></p>
---	---

Cette modification permet de préciser la manière par laquelle chaque accès aux images est archivé par le système. Cette procédure est déjà implémentée dans le système que nous utilisons actuellement.

<p><b>Art. 5 Traitement des données</b></p> <p>Les images enregistrées ne peuvent être visionnées qu'en cas d'infraction <del>ou d'événements graves demandant une intervention ou faisant l'objet d'une plainte</del>. Elles ne peuvent être traitées que pour atteindre le but fixé pour les installations de vidéosurveillance.</p> <p>Les images ne peuvent être transmises qu'aux autorités chargées de poursuivre les infractions constatées.</p>	<p><b>Art. 5 Traitement des données</b></p> <p>Les images enregistrées ne peuvent être visionnées qu'en cas d'infraction. Elles ne peuvent être traitées que pour atteindre le but fixé pour les installations de vidéosurveillance.</p> <p>Les images ne peuvent être transmises qu'aux autorités chargées de poursuivre les infractions constatées.</p>
---	---

Cette modification allège l'article dont la version actuelle faisait inutilement mention de synonymes au terme « infraction ».

<p><b>Art. 9 Durée de conservation</b></p> <p>La durée de conservation des images ne peut excéder <del>96 heures</del>, sauf si les données sont transmises conformément à l'article 5 alinéa 2.</p> <p>Les images sont détruites automatiquement à la fin du délai de conservation.</p>	<p><b>Art. 9 Durée de conservation</b></p> <p>La durée de conservation des images ne peut excéder <u>les délais prévus par la LPrD</u>, sauf si les données sont transmises conformément à l'article 5 alinéa 2.</p> <p>Les images sont détruites automatiquement à la fin du délai de conservation.</p>
--	--

Cette modification permet d'étendre la durée maximale de conservation des images en la portant à 7 jours ou, en cas d'atteinte aux personnes ou aux biens, à 100 jours. A l'issue de ce délai, les images seraient, comme actuellement, automatiquement détruites par le système.

## 4. Conclusions

Vu ce qui précède, la Municipalité vous prie, Monsieur le Président, Mesdames et Messieurs les Conseillères et Conseillers, de bien vouloir prendre les décisions suivantes :

- vu le préavis municipal n° 17-2018 du 22 octobre 2018,
- où le rapport de la commission chargée de rapporter sur cet objet,
- considérant que cet objet est porté à l'ordre du jour,

le Conseil communal de Cugy (VD) décide :

- d'approuver la révision partielle du Règlement communal relatif à l'utilisation de caméras de vidéosurveillance dissuasive conformément au projet annexé au présent préavis ;
- de mettre en vigueur les dispositions révisées et les nouvelles dispositions du Règlement communal relatif à l'utilisation de caméras de vidéosurveillance dissuasive dès son approbation par le/la Chef/fe du Département concerné.

Ainsi approuvé par la Municipalité dans sa séance du 22 octobre 2018 pour être soumis à l'approbation du Conseil communal.

Au nom de la Municipalité

Le syndic

Le secrétaire

T. Amy

P. Csikos

Municipal en charge du dossier : M. Thierry Amy, syndic

Annexes : - 1 - Règlement communal relatif à l'utilisation de caméras de vidéosurveillance dissuasive amendé avec modifications proposées des articles 1, 4, 5, et 9.  
- 2 - Loi sur la protection des données personnelles du 11 septembre 2007 (LPrD ; RSV 172.65).  
- 3 - Loi modifiant celle du 11 septembre 2007 sur la protection des données personnelles du 5 juin 2018, publié dans la FAO du 19 juin 2018.  
- 4 - Arrêté de mise en vigueur du 5 septembre 2018, publié dans la FAO du 11 septembre 2018.



# **COMMUNE DE CUGY VD**

---

## **Règlement communal relatif à l'utilisation de caméras de vidéosurveillance dissuasive**

---

# Règlement communal relatif à l'utilisation de caméras de vidéosurveillance dissuasive

---

Vu les articles 22 et 23 de la loi du 11 septembre 2007 sur la protection des données personnelles

Vu les articles 9 et 10 du règlement du 29 octobre 2008 d'application de la loi sur la protection des données personnelles

## Article premier – Principe

Un système de vidéosurveillance dissuasive peut, après avoir obtenu l'autorisation ~~du Préposé à la protection des données et à l'information de l'autorité compétente~~, être installé sur le domaine public ou le patrimoine administratif communal dans le but d'éviter la perpétration d'infractions contre des personnes et des biens et d'apporter des moyens de preuve en cas de telles infractions. Il doit constituer, si possible en complément d'autres mesures, le moyen le plus adéquat pour atteindre le but fixé.

## Art. 2 Délégation

La Municipalité est compétente pour adopter un règlement portant sur le but et les modalités des installations de vidéosurveillance, ainsi que sur les lieux sur lesquels elles sont mises en œuvre et déploient leurs effets.

## Art. 3 Installations

Pour chaque installation, la Municipalité détermine l'emplacement et le champ des caméras, qui doivent se limiter à la mesure nécessaire pour atteindre le but fixé, en limitant les atteintes aux droits des personnes concernées.

## Art. 4 Sécurité des données

Des mesures de sécurité appropriées sont prises afin d'éviter tout traitement illicite des données, notamment en limitant l'accès aux données enregistrées et aux locaux qui les contiennent.

~~Le contrôle des accès aux images sera garanti.~~ Un système de journalisation automatique permet de contrôler les accès aux images.

## Art. 5 Traitement des données

Les images enregistrées ne peuvent être visionnées qu'en cas d'infraction ~~ou d'événements graves demandant une intervention ou faisant l'objet d'une plainte~~. Elles ne peuvent être traitées que pour atteindre le but fixé pour les installations de vidéosurveillance.

Les images ne peuvent être transmises qu'aux autorités chargées de poursuivre les infractions constatées.

## Art. 6 Personnes responsables

La Municipalité désigne la ou les personnes autorisées à gérer l'installation de vidéosurveillance et à visionner les images.

La ou les personnes responsables prennent les mesures nécessaires pour prévenir tout traitement illicite; elles s'assurent du respect des mesures de sécurité et des dispositions en matière de protection des données et en rendent compte à la Municipalité.

### **Art. 7 Information**

Les personnes se trouvant dans la zone surveillée doivent être informées de la vidéosurveillance par des panneaux d'information.

La Municipalité tient une liste publique et tenue à jour des installations de vidéosurveillance exploitées sur la base du présent règlement.

### **Art. 8 Horaire de fonctionnement**

L'horaire de fonctionnement des installations est décidé par la Municipalité en fonction des nécessités pour atteindre le but fixé.

### **Art. 9 Durée de conservation**

La durée de conservation des images ne peut excéder ~~96 heures~~ les délais prévus par la LPrD, sauf si les données sont transmises conformément à l'article 5 alinéa 2.

Les images sont détruites automatiquement à la fin du délai de conservation.

Adopté en séance de Municipalité le 6 février 2013

#### AU NOM DE LA MUNICIPALITE

Le Syndic

La secrétaire

R. Bron

M. P. Durussel

Adopté par le Conseil communal le 21 mars 2013

#### AU NOM DU CONSEIL COMMUNAL

Le Président

La secrétaire

Th. Amy

V. Seivel

Approuvé par la Cheffe du Département de l'intérieur, le 1<sup>er</sup> mai 2013

Modifications des articles 1, 4, 5, 9 adoptées par la Municipalité lors de sa séance du 22 octobre 2018.

Le Syndic :

Le Secrétaire

T. Amy

P. Csikos

Modifications des articles 1, 4, 5, 9 adoptées par le Conseil communal lors de sa séance du ...

Le Président :

Le Secrétaire :

S. Debossens

Z. Stanimirovic

Modifications des articles 1, 4, 5, 9 approuvées par la Cheffe du Département des institutions et de la sécurité le ...



# LOI

## sur la protection des données personnelles (LPrD)

du 11 septembre 2007

LE GRAND CONSEIL DU CANTON DE VAUD

vu l'article 15 de la Constitution cantonale du 14 avril 2003 <sup>A</sup>

vu le projet de loi présenté par le Conseil d'Etat

décrète

### Chapitre I But, champ d'application et définitions

#### Art. 1 But

<sup>1</sup> La présente loi vise à protéger les personnes contre l'utilisation abusive des données personnelles les concernant.

#### Art. 2 Terminologie

<sup>1</sup> La désignation des fonctions s'applique indifféremment aux femmes et aux hommes.

#### Art. 3 Champ d'application<sup>4</sup>

<sup>1</sup> La présente loi s'applique à tout traitement de données des personnes physiques ou morales.

<sup>2</sup> Sont soumis à la présente loi les entités suivantes :

- a. le Grand Conseil ;
- b. le Conseil d'Etat et son administration ;
- c. l'Ordre judiciaire et son administration ;
- cbis. la Cour des comptes ;
- d. les communes, ainsi que les ententes, associations, fédérations, fractions et agglomérations de communes ;
- e. les personnes physiques et morales auxquelles le canton ou une commune confie des tâches publiques, dans l'exécution desdites tâches.

<sup>3</sup> La présente loi ne s'applique pas :

- a. aux délibérations du Grand Conseil et des conseils généraux et communaux ;
- b. aux procédures civiles, pénales ou administratives ;
- c. aux données personnelles traitées en application de la loi fédérale sur le renseignement et de l'article 2, alinéa 1 de la loi sur les dossiers de police judiciaire.

#### Art. 4 Définitions

<sup>1</sup> On entend par :

1. *Donnée personnelle*, toute information qui se rapporte à une personne identifiée ou identifiable ;
2. *Donnée sensible*, toute donnée personnelle se rapportant :
  - aux opinions ou activités religieuses, philosophiques, politiques ou syndicales, ainsi qu'à une origine ethnique ;
  - à la sphère intime de la personne, en particulier à son état psychique, mental ou physique ;
  - aux mesures et aides individuelles découlant des législations sociales ;
  - aux poursuites ou sanctions pénales et administratives.
3. *Profil de la personnalité*, assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique ;
4. *Personne concernée*, toute personne physique ou morale au sujet de laquelle les données sont traitées ;
5. *Traitement de données personnelles*, toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données personnelles, notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ;
6. *Communication*, fait de rendre des données accessibles, notamment de les transmettre, les publier, autoriser leur consultation ou fournir des renseignements ;

7. *Fichier*, tout ensemble structuré de données personnelles accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;
8. *Responsable du traitement*, personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine le contenu, ainsi que les finalités du fichier ;
9. *Sous-traitant*, personne physique ou morale, autorité publique ou tout autre organisme qui traite des données personnelles pour le compte du responsable du traitement ;
10. *Procédure d'appel*, mode de communication automatisé des données par lequel les destinataires décident eux-mêmes de la communication des données, moyennant une autorisation du responsable du traitement ;
11. *Destinataire*, personne physique ou morale, de droit privé ou de droit public, qui reçoit communication de données, qu'il s'agisse ou non d'un tiers. Les autorités qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière ne sont toutefois pas considérées comme des destinataires ;
12. *Entités*, entités décrites à l'article 3, alinéa 2 de la présente loi ;
13. *Loi au sens formel*, lois au sens formel adoptées par le Grand Conseil ou, sur le plan communal, règlements adoptés par les conseils généraux et communaux ;
14. *Vidéosurveillance dissuasive*, vidéosurveillance à laquelle on recourt pour éviter la perpétration d'infractions sur un certain lieu.

## Chapitre II Dispositions générales

### SECTION I PRINCIPES

#### Art. 5 Légalité

<sup>1</sup> Les données personnelles ne peuvent être traitées que si :

- a. une base légale l'autorise ou
- b. leur traitement sert à l'accomplissement d'une tâche publique.

<sup>2</sup> Les données sensibles ne peuvent être traitées que si :

- a. une loi au sens formel le prévoit expressément,
- b. l'accomplissement d'une tâche clairement définie dans une loi au sens formel l'exige absolument, ou
- c. la personne concernée y a consenti ou a rendu ses données accessibles à tout un chacun.

#### Art. 6 Finalité

<sup>1</sup> Les données ne doivent être traitées que dans le but indiqué lors de leur collecte, tel qu'il ressort de la loi ou de l'accomplissement de la tâche publique concernée.

#### Art. 7 Proportionnalité

<sup>1</sup> Le traitement des données personnelles doit être conforme au principe de la proportionnalité.

#### Art. 8 Transparence

<sup>1</sup> La collecte des données personnelles doit être reconnaissable pour la personne concernée.

#### Art. 9 Exactitude

<sup>1</sup> Les entités soumises à la présente loi s'assurent que les données personnelles traitées sont exactes.

#### Art. 10 Sécurité

<sup>1</sup> Le responsable du traitement prend les mesures appropriées pour garantir la sécurité des fichiers et des données personnelles, soit notamment contre leur perte, leur destruction, ainsi que tout traitement illicite.

#### Art. 11 Conservation

<sup>1</sup> Les données personnelles doivent être détruites ou rendues anonymes dès qu'elles ne sont plus nécessaires à la réalisation de la tâche pour laquelle elles ont été collectées.

<sup>2</sup> Demeurent réservées les dispositions légales spécifiques à la conservation des données, en particulier à leur archivage, ou effectuées à des fins historiques, statistiques ou scientifiques.

#### Art. 12 Consentement

<sup>1</sup> Lorsque le traitement de données personnelles requiert le consentement de la personne concernée, cette dernière ne consent valablement que si elle exprime sa volonté librement et après avoir été dûment informée. Lorsqu'il s'agit de données sensibles et de profil de la personnalité, son consentement doit être au surplus explicite.

### SECTION II TRAITEMENT DES DONNÉES PERSONNELLES

#### Art. 13 Devoir d'informer

<sup>1</sup> Le responsable du traitement informe la personne concernée de toute collecte des données personnelles la concernant.

<sup>2</sup> Les informations fournies à la personne concernée sont les suivantes :

- a. l'identité du responsable du traitement ;
- b. la finalité du traitement pour lequel les données sont collectées ;
- c. au cas où la communication des données est envisagée, les catégories des destinataires des données ;
- d. le droit d'accéder aux données ;
- e. la possibilité de refuser de fournir les données requises et les conséquences d'un tel refus.

<sup>3</sup> Si les données ne sont pas collectées auprès de la personne concernée, le responsable du traitement doit fournir par écrit à cette dernière les informations énumérées à l'alinéa précédent, au plus tard lors de l'enregistrement des données, à moins que cela ne s'avère impossible, ne nécessite des efforts disproportionnés ou que l'enregistrement ou la communication ne soient expressément prévus par la loi.

#### **Art. 14 Restriction du devoir d'information**

<sup>1</sup> Le responsable du traitement peut différer, restreindre, voire refuser l'information, dans la mesure où :

- a. la loi le prévoit expressément ;
- b. un intérêt public ou privé prépondérant l'exige ;
- c. l'information ou la communication du renseignement risque de compromettre une instruction pénale ou une autre procédure d'instruction, ou
- d. l'information requise ne peut objectivement être fournie.

<sup>2</sup> Dès que le motif justifiant la restriction du devoir d'information disparaît, le responsable du traitement doit fournir l'information, à moins que cela ne soit impossible ou ne nécessite des efforts disproportionnés.

#### **Art. 15 Communication**

<sup>1</sup> Les données personnelles peuvent être communiquées par les entités soumises à la présente loi lorsque :

- a. une disposition légale au sens de l'article 5 le prévoit ;
- b. le requérant établit qu'il en a besoin pour accomplir ses tâches légales ;
- c. le requérant privé justifie d'un intérêt prépondérant à la communication primant celui de la personne concernée à ce que les données ne soient pas communiquées ;
- d. la personne concernée a expressément donné son consentement ou les circonstances permettent de présumer ledit consentement ;
- e. la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas formellement opposée à leur communication ; ou
- f. le requérant rend vraisemblable que la personne concernée ne refuse son accord que dans le but de l'empêcher de se prévaloir de prétentions juridiques ou de faire valoir d'autres intérêts légitimes ; dans ce cas, la personne concernée est invitée, dans la mesure du possible, à se prononcer, préalablement à la communication des données.

<sup>2</sup> L'alinéa 1 est également applicable aux informations transmises sur demande en vertu de la loi sur l'information.

<sup>3</sup> Les autorités peuvent communiquer spontanément des données personnelles dans le cadre de l'information au public, en vertu de la loi sur l'information <sup>A</sup>, à condition que la communication réponde à un intérêt public ou privé prévalant sur celui de la personne concernée.

#### **Art. 16 Procédure d'appel<sup>4</sup>**

<sup>1</sup> Les données peuvent être rendues accessibles au moyen d'une procédure d'appel entre les entités soumise à la loi aux conditions de l'article 15. Les données sensibles ou les profils de la personnalité ne peuvent être rendus accessibles au moyen d'une procédure d'appel que si une loi au sens formel ou un règlement le prévoit.

<sup>2</sup> Les données ne peuvent être rendues accessibles à des personnes privées au moyen d'une procédure d'appel que si une loi au sens formel ou un règlement le prévoit. Les données sensibles ou les profils de la personnalité ne peuvent être rendus accessibles que si une loi au sens formel le prévoit expressément.

#### **Art. 17 Communication transfrontière de données**

<sup>1</sup> La communication vers un pays tiers de données personnelles faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement, ne peut avoir lieu que si le pays tiers en question assure un niveau de protection adéquat.

<sup>2</sup> L'alinéa précédent n'est pas applicable :

- a. si la personne concernée a donné son consentement, qui doit dans tous les cas être explicite ;
- b. si la communication de données est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures pré-contractuelles prises à la demande de la personne concernée ;
- c. si la communication est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ;
- d. si la communication est, en l'espèce, indispensable soit à la sauvegarde d'un intérêt public, soit à la constatation, l'exercice ou la défense d'un droit en justice ;
- e. si la communication est, en l'espèce nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ;

- f. si la communication intervient d'un registre public qui, en vertu de dispositions légales ou réglementaires, est destiné à l'information du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier ;
- g. si des garanties suffisantes, notamment contractuelles, permettent d'assurer un niveau de protection adéquat à l'étranger.

#### **Art. 18 Traitement des données par un tiers**

<sup>1</sup> Le traitement de données peut être confié à un tiers aux conditions cumulatives suivantes :

- a. le traitement par un tiers est prévu par la loi ou par un contrat ;
- b. le responsable du traitement est légitimé à traiter lui-même les données concernées ;
- c. aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

<sup>2</sup> Le tiers est responsable de la sécurité des données qu'il traite.

### **Chapitre III Fichiers**

#### **Art. 19 Registre des fichiers**

<sup>1</sup> Le Préposé cantonal à la protection des données et à l'information (ci-après : le Préposé) tient un registre des fichiers, qui est public et accessible en ligne.

<sup>2</sup> Le Conseil d'Etat édicte les règles applicables à la tenue du registre <sup>A</sup>.

#### **Art. 20 Annonce**

<sup>1</sup> Les entités soumises à la présente loi sont tenues d'informer sans délai le Préposé lors de tout projet visant à constituer un nouveau fichier contenant des données personnelles.

<sup>2</sup> Le Conseil d'Etat fixe les renseignements à fournir lors de l'annonce de fichier.

#### **Art. 21 Mise en service**

<sup>1</sup> Les fichiers peuvent être opérationnels dès que le Préposé a été informé de leur constitution.

#### **Art. 21a Exceptions<sup>4</sup>**

<sup>1</sup> N'ont pas à être déclarés, s'ils ne contiennent pas de données sensibles ou ne constituent pas un profil de la personnalité :

- a. les fichiers renfermant uniquement des informations accessibles au public ;
- b. les fichiers d'enregistrement de la correspondance ;
- c. les fichiers d'adresses ;
- d. les fichiers éphémères dont la durée de vie n'excède pas un an.

### **Chapitre IV Vidéosurveillance**

#### *SECTION I DISPOSITIONS GÉNÉRALES ET PROCÉDURE D'AUTORISATION<sup>4</sup>*

#### **Art. 22 Principes<sup>4</sup>**

<sup>1</sup> Les entités citées à l'article 3, alinéa 2 peuvent installer un système de vidéosurveillance dissuasive, avec ou sans système d'enregistrement, sur le domaine public ou leur patrimoine affecté à la réalisation d'une tâche publique, moyennant le respect des principes et prescriptions de la présente loi.

<sup>1bis</sup> Les buts d'un système de vidéosurveillance dissuasive sont de garantir la sécurité des personnes et des biens, d'éviter la perpétration d'infractions sur un certain lieu et de contribuer à la poursuite et à la répression d'infractions.

<sup>2</sup> ...

<sup>3</sup> ...

<sup>4</sup> L'installation du système de vidéosurveillance doit constituer le moyen le plus adéquat pour atteindre le but poursuivi. Toutes les mesures doivent être prises pour limiter les atteintes aux personnes concernées.

<sup>5</sup> ...

<sup>6</sup> ...

<sup>7</sup> Le Conseil d'Etat précise les conditions précitées.

#### **Art. 22a Autorisation<sup>4</sup>**

<sup>1</sup> Préalablement à son exploitation, l'installation de vidéosurveillance doit faire l'objet d'une demande d'autorisation du responsable du traitement. Il en va de même pour toute modification ultérieure du système.

<sup>2</sup> L'autorité compétente peut demander l'avis du Préposé avant de statuer. Le Préposé reçoit une copie de la décision.

<sup>3</sup> Si un système ne remplit plus les conditions légales, l'autorisation est retirée.

<sup>4</sup> Le Préposé publie une liste des installations de vidéosurveillance dissuasive qui ont été autorisées.

<sup>5</sup> Le Conseil d'Etat précise dans un règlement la procédure d'autorisation.

**Art. 22b Autorités compétentes<sup>4</sup>**

<sup>1</sup> Lorsque la demande émane d'une entité cantonale, l'autorité compétente est le chef du département dont dépend l'entité concernée.

<sup>2</sup> Lorsque la demande émane d'une entité communale, l'autorité compétente est le préfet du district.

<sup>3</sup> Lorsque la demande émane d'un établissement de droit public cantonal ou d'une personne morale à laquelle le canton a confié des tâches publiques, l'autorité compétente est l'organe suprême de l'établissement.

**Art. 22c Recours<sup>4</sup>**

<sup>1</sup> Le Préposé a la qualité pour recourir contre une décision d'autorisation auprès du Tribunal cantonal.

<sup>2</sup> Le responsable du traitement a la qualité pour recourir contre une décision de refus d'autorisation auprès du Tribunal cantonal.

**Art. 23a Durée de conservation des images<sup>4</sup>**

<sup>1</sup> A moins qu'une autorité n'ordonne leur conservation dans le cadre d'une procédure pénale, les images enregistrées doivent être détruites automatiquement après un délai de sept jours, ou en cas d'atteinte aux personnes ou aux biens, après cent jours au maximum.

**Art. 23b Délégation<sup>4</sup>**

<sup>1</sup> L'exploitation d'une installation de vidéosurveillance peut être déléguée à un tiers aux conditions de l'article 18.

<sup>2</sup> La délégation fait l'objet d'une décision d'autorisation en application de la procédure prévue aux articles 22a et 22b.

<sup>3</sup> Le responsable du traitement procède à des contrôles réguliers afin de s'assurer que les conditions légales sont respectées.

**Art. 23c Autorisation cadre<sup>4</sup>**

<sup>1</sup> Si les besoins spécifiques d'une entité mentionnée à l'article 3, alinéa 2, lettres a à c<sup>bis</sup> le justifient, l'autorité compétente peut délivrer une autorisation de principe, dite autorisation cadre, permettant à l'entité bénéficiaire d'installer et d'exploiter, aux conditions définies par l'autorisation cadre, plusieurs installations de vidéosurveillance.

<sup>2</sup> Pour toute installation d'un système de vidéosurveillance, l'entité cantonale au bénéfice d'une autorisation cadre en informe l'autorité compétente et le Préposé.

<sup>3</sup> Le Conseil d'Etat précise dans un règlement les conditions d'octroi d'une autorisation cadre.

**Art. 23d Sécurité des données<sup>4</sup>**

<sup>1</sup> Le responsable du traitement prend les mesures de sécurité appropriées afin de protéger les données enregistrées ou en transfert sur les réseaux informatiques et d'éviter tout traitement illicite de celles-ci. Il limite notamment l'accès aux données et aux locaux qui les contiennent.

<sup>2</sup> Il doit installer et maintenir un système de journalisation automatique permettant de contrôler les accès aux images.

**Art. 23e Traitement des données<sup>4</sup>**

<sup>1</sup> L'accès aux images est limité aux personnes désignées par le responsable de traitement, ainsi qu'à celles qui peuvent se prévaloir d'un droit d'accès à leurs propres données, au sens du chapitre VI.

<sup>2</sup> Le responsable de traitement définit la procédure à suivre pour les opérations techniques de gestion des systèmes et des données informatiques liées à la vidéosurveillance.

<sup>3</sup> En vue d'obtenir des moyens de preuve, les images enregistrées peuvent être analysées en cas de dénonciation pénale, de plainte pénale ou d'indices concrets de la commission d'un acte pénalement punissable.

<sup>4</sup> Le responsable du traitement ne peut transmettre les images enregistrées qu'aux autorités chargées de poursuivre l'infraction pénale.

**SECTION II DISPOSITIONS SPÉCIALES<sup>4</sup>****Art. 23f Communes<sup>4</sup>**

<sup>1</sup> Outre le respect des conditions posées à la section précédente, l'installation d'un système de vidéosurveillance sur le domaine public et le patrimoine affecté à la réalisation d'une tâche publique communale ou intercommunale nécessite l'adoption d'un règlement communal ou intercommunal.

<sup>2</sup> Les images enregistrées par le système de vidéosurveillance ne peuvent être utilisées que selon les modalités, aux conditions et aux fins fixées dans le règlement qui l'institue.

<sup>3</sup> Ce règlement ne peut déroger aux conditions minimales fixées par la loi.

**Art. 23g Etablissements scolaires<sup>4</sup>**

<sup>1</sup> L'installation d'un système de vidéosurveillance dans ou aux abords immédiats d'un établissement scolaire communal ou intercommunal nécessite, outre l'autorisation prévue à l'article 22a, l'approbation du département chargé de la formation.

**Art. 23h Etablissements pénitentiaires<sup>4</sup>**

<sup>1</sup> Les établissements pénitentiaires peuvent installer un système de vidéosurveillance de sécurité.

<sup>2</sup> Le Conseil d'Etat fixe les conditions à respecter quant à l'exploitation d'un système de vidéosurveillance de sécurité.

<sup>3</sup> Au surplus, les dispositions du présent chapitre ne s'appliquent pas à la vidéosurveillance dans les établissements pénitentiaires.

## Chapitre V Statistiques, planification et recherche

### Art. 24

<sup>1</sup> Les entités soumises à la présente loi sont en droit de traiter des données personnelles et de les communiquer à des fins de recherche, de la planification ou de la statistique, aux conditions suivantes :

- a. elles sont rendues anonymes dès que le but de leur traitement le permet ;
- b. le destinataire ne communique les données à des tiers qu'avec le consentement de l'entité qui les lui a transmises ;
- c. les résultats du traitement sont publiés sous une forme ne permettant pas d'identifier les personnes concernées.

<sup>2</sup> Les articles 5, 6, 15 de la présente loi ne sont pas applicables.

<sup>3</sup> La loi sur la statistique cantonale <sup>A</sup>est pour le surplus applicable.

## Chapitre VI Droits de la personnes concernée

### Art. 25 Droit d'accès à ses propres données<sup>4</sup>

<sup>1</sup> Toute personne a, en tout temps, libre accès aux données la concernant.

<sup>2</sup> Elle peut également requérir du responsable du traitement la confirmation qu'aucune donnée la concernant n'a été collectée.

<sup>3</sup> La personne qui fait valoir son droit doit justifier de son identité.

<sup>4</sup> Nul ne peut renoncer par avance au droit d'accès.

### Art. 26 Modalités

<sup>1</sup> La demande portant sur la communication de données personnelles n'est soumise à aucune exigence de forme. Elle doit toutefois contenir les indications suffisantes pour permettre d'identifier la donnée concernée.

<sup>2</sup> La communication de données a lieu sur place ou se fait par écrit, sauf disposition contraire.

<sup>3</sup> Avec l'accord du requérant, la communication peut également se faire par oral.

<sup>4</sup> La communication des données est, en règle générale, gratuite.

<sup>5</sup> Le responsable du traitement qui répond à la demande peut percevoir un émoluments :

- a. lorsque la communication requiert un travail important ;
- b. en cas de demandes répétitives ;
- c. lorsqu'une copie est demandée.

<sup>6</sup> Le Conseil d'Etat fixe le tarif des émoluments.

### Art. 26a Délais<sup>4</sup>

<sup>1</sup> Le responsable de traitement répond dans les trente jours à compter de la date de réception de la demande par l'entité concernée.

### Art. 27 Restrictions

<sup>1</sup> Le responsable du traitement peut restreindre la consultation, voire refuser celle-ci, si :

- a. la loi le prévoit expressément ;
- b. un intérêt public ou privé prépondérant l'exige ;
- c. elle est impossible ou nécessite des efforts disproportionnés.

<sup>2</sup> Le droit d'accès aux données médicales est régi par la loi sur la santé publique <sup>A</sup>.

<sup>3</sup> Dès que le motif justifiant la restriction du devoir d'accès disparaît, le responsable du traitement doit fournir l'information.

### Art. 28 Droit d'opposition

<sup>1</sup> Toute personne a le droit de s'opposer à ce que les données personnelles la concernant soient communiquées, si elle rend vraisemblable un intérêt digne de protection.

<sup>2</sup> Le responsable du traitement rejette ou lève l'opposition :

- a. si la communication est expressément prévue par une disposition légale ;
- b. si la communication est indispensable à l'accomplissement des tâches publiques du destinataire des données et prime les intérêts de la personne concernée.

### Art. 29 Autres droits

<sup>1</sup> Les personnes qui ont un intérêt digne de protection peuvent exiger du responsable du traitement qu'il :

- a. s'abstienne de procéder à un traitement illicite de données
- b. supprime les effets d'un traitement illicite de données ;

- c. constate le caractère illicite d'un traitement de données ;
- d. répare les conséquences d'un traitement illicite de données.

<sup>2</sup> Le cas échéant, elles peuvent demander au responsable du traitement de :

- a. rectifier, détruire les données ou les rendre anonymes ;
- b. publier ou communiquer à des tiers la décision ou la rectification.

<sup>3</sup> Si ni l'exactitude, ni l'inexactitude d'une donnée ne peut être établie, le responsable du traitement ajoute à la donnée la mention de son caractère litigieux.

## Chapitre VII Procédure

### Art. 30 Décision du responsable du traitement

<sup>1</sup> Pour toute demande fondée sur la présente loi, notamment sur les articles 25 à 29, le responsable du traitement rend une décision comprenant les motifs l'ayant conduit à ne pas y donner suite.

<sup>2</sup> Le responsable du traitement adresse une copie de sa décision au Préposé.

### Art. 31 Recours

a) En général <sup>3</sup>

<sup>1</sup> L'intéressé peut recourir au Préposé, ou directement au Tribunal cantonal.

<sup>2</sup> Au surplus, la loi sur la procédure administrative <sup>A</sup>est applicable aux décisions rendues en vertu de la présente loi, ainsi qu'aux recours contre dites décisions.

### Art. 32 b) Recours au Préposé et conciliation <sup>1, 2, 4</sup>

<sup>1</sup> Dès qu'il est saisi du recours, le Préposé le notifie au responsable du traitement.

<sup>2</sup> Le Préposé tente la conciliation afin d'amener les parties à un accord. Il dispose à cet effet des moyens décrits à l'article 38 de la présente loi.

<sup>3</sup> Si la conciliation aboutit, l'affaire est classée.

<sup>4</sup> En cas d'échec de la conciliation, le Préposé rend une décision qu'il notifie au responsable du traitement et à l'intéressé.

<sup>5</sup> Le responsable du traitement et l'intéressé peuvent recourir au Tribunal cantonal dans un délai de 30 jours dès la notification.

### Art. 33 Gratuité <sup>3</sup>

<sup>1</sup> La procédure est gratuite.

<sup>2</sup> Un émolument peut être perçu en cas de demande abusive.

<sup>3</sup> ...

## Chapitre VIII Préposé cantonal à la protection des données et à l'information

### Art. 34 Désignation

<sup>1</sup> Le Préposé est désigné par le Conseil d'Etat, pour une période de 6 ans.

<sup>2</sup> Son mandat est renouvelable.

### Art. 35 Statut et rattachement <sup>4</sup>

<sup>1</sup> Le Préposé exerce son activité de manière indépendante.

<sup>2</sup> Le Conseil d'Etat décide de son rattachement administratif.

<sup>3</sup> Le Préposé est tenu au secret de fonction.

### Art. 36 Tâches <sup>4</sup>

1. Surveillance

<sup>1</sup> Le Préposé surveille l'application des prescriptions relatives à la protection des données.

<sup>2</sup> A cette fin, il dispose des moyens prévus à l'article 38 de la présente loi.

<sup>3</sup> S'il estime que les prescriptions sur la protection des données ont été violées, le Préposé transmet une recommandation à l'entité concernée, en vue de modifier ou cesser le traitement concerné.

<sup>4</sup> L'entité concernée prend position par écrit. Si la recommandation du Préposé n'est pas suivie, ce dernier peut porter l'affaire devant le département ou l'entité concernée, pour décision.

<sup>5</sup> Le Préposé peut recourir contre la décision rendue conformément à l'alinéa précédent, ainsi que contre la décision rendue par l'autorité compétente (article 30). La loi sur la procédure administrative <sup>A</sup>est applicable.

<sup>6</sup> Les rapports d'audit établis par le Préposé en application des dispositions qui précèdent sont communiqués au Président du Conseil d'Etat et au Président de la Commission de gestion du Grand Conseil.

**Art. 37** 2. Autres tâches<sup>4</sup>

<sup>1</sup> Outre la surveillance mentionnée ci-dessus, le Préposé :

- a. promeut la protection des données dans le canton ;
- b. informe les responsables de traitement sur les exigences posées en matière de protection des données ;
- c. renseigne les personnes concernées sur les droits découlant de la présente loi ;
- d. est consulté lors de l'élaboration de loi, règlement, directive ou autre norme impliquant le traitement de données personnelles ;
- e. intervient, sur demande des responsables de traitement ou des personnes concernées, afin de résoudre des questions soumises à la présente loi, le recours prévu aux articles 30 à 33 de la présente loi étant réservé ;
- f. peut être consulté sur les projets relatifs à l'installation de systèmes de vidéosurveillance et dispose en cette matière d'un droit de recours, conformément aux articles 22 et suivants de la présente loi ;
- g. tient à jour le Registre des fichiers institué à l'article 19 de la présente loi ;
- h. collabore avec les autres autorités compétentes en matière de protection des données des autres cantons, de la Confédération ou de l'étranger.

<sup>2</sup> En outre, le Préposé connaît des recours prévus à l'article 31 de la présente loi.

**Art. 38 Moyens**

<sup>1</sup> Dans le cadre de ses tâches, le Préposé peut :

- a. accéder aux données faisant l'objet d'un traitement et recueillir toutes les informations nécessaires à l'accomplissement de ses tâches ;
- b. rendre un préavis préalablement à la mise en œuvre d'un fichier ;
- c. demander au responsable du traitement de restreindre ou cesser immédiatement, de manière temporaire ou définitive, le traitement de données personnelles, si des intérêts dignes de protection de la personne concernée le requièrent.

**Art. 39 Obligation de renseigner**

<sup>1</sup> Le responsable du traitement est tenu d'assister le Préposé dans l'accomplissement de ses tâches. A cet effet, il lui fournit les informations ou pièces nécessaires et le laisse accéder à ses locaux.

<sup>2</sup> Le secret de fonction ne peut être opposé au Préposé.

<sup>3</sup> Les tiers sont également tenus de fournir les renseignements requis par le Préposé.

**Art. 40 Rapport<sup>4</sup>**

<sup>1</sup> Le Préposé établit chaque année un rapport d'activité.

<sup>2</sup> Ce rapport est public. Il renseigne notamment sur les recommandations prévues à l'article 36, alinéa 3 adressées dans l'année et, le cas échéant, sur les démarches entreprises par le Préposé en application de l'article 36, alinéas 4 et 5.

<sup>3</sup> Le Préposé peut établir, en tout temps, un rapport spécial, d'office ou sur demande du Grand Conseil ou du Conseil d'Etat.

**Chapitre IX Dispositions finales<sup>4</sup>****Art. 41 Violation du devoir de discrétion<sup>4</sup>**

<sup>1</sup> Toute personne ayant révélé intentionnellement, d'une manière illicite, des données personnelles ou sensibles qui ont été portées à sa connaissance dans l'exercice de sa fonction, sera punie d'une amende.

<sup>2</sup> Est passible de la même peine la personne ayant révélé intentionnellement, d'une manière illicite, des données personnelles ou sensibles portées à sa connaissance dans le cadre des activités qu'elle exerce pour le compte de personnes soumises à l'obligation de garder le secret.

<sup>3</sup> L'obligation de discrétion persiste au-delà de la fin des rapports de travail.

<sup>3bis</sup> Celui qui met en place une installation de vidéosurveillance sans en avoir au préalable demandé l'autorisation ou qui exploite une installation de vidéosurveillance sans en respecter les conditions légales sera puni de l'amende.

<sup>4</sup> Le droit pénal fédéral est réservé.

**Chapitre X Dispositions transitoires et finales****Art. 42 Application de la loi<sup>4</sup>**

<sup>1</sup> Tout traitement des données doit se conformer à la présente loi, notamment en matière de légalité, dans les cinq ans suivant son entrée en vigueur.



2 ...

<sup>3</sup> Tout système de vidéosurveillance dissuasive installé par les entités cantonales, les établissements de droit public, et les personnes morales auxquelles le canton a confié des tâches publiques, doit se conformer aux dispositions du chapitre IV de la présente loi dans un délai d'un an suivant l'entrée en vigueur de la loi du 5 juin 2018 modifiant la loi du 11 septembre 2007 sur la protection des données personnelles ; toutefois, les règles relatives à la durée de conservation des images sont immédiatement applicables.

<sup>4</sup> Toute modification d'un système de vidéosurveillance communal, autorisé avant l'entrée en vigueur de la loi du 5 juin 2018 modifiant la loi du 11 septembre 2007 sur la protection des données personnelles, est soumise à la procédure d'autorisation prévue au chapitre IV de la présente loi.

**Art. 43**<sup>4</sup> ...

**Art. 44**

<sup>1</sup> La loi du 25 mai 1981 sur les fichiers informatiques et la protection des données personnelles est abrogée.

**Art. 45**

<sup>1</sup> Le Conseil d'Etat est chargé de l'exécution de la présente loi. Il en publiera le texte conformément à l'article 84, alinéa 1, lettre a) de la Constitution cantonale et en fixera, par voie d'arrêté, la date d'entrée en vigueur.

## **Chapitre XI Dispositions transitoires de la loi du 5 juin 2018**

**Art. 46**

<sup>1</sup> Les demandes d'autorisations déposées avant l'entrée en vigueur de la loi du 5 juin 2018 modifiant la présente loi, et pour lesquelles une décision d'autorisation n'a pas encore été rendue, sont soumises à la procédure des articles 22 et suivants de la loi du 11 septembre 2007 sur la protection des données personnelles.

Entrée en vigueur : 01.11.2008



---

**LOI 172.65**  
**modifiant celle du 11 septembre 2007 sur la protection**  
**des données personnelles**du 5 juin 2018

---

LE GRAND CONSEIL DU CANTON DE VAUD

vu le projet de loi présenté par le Conseil d'Etat

*décète***Article premier**

<sup>1</sup> La loi du 11 septembre 2007 sur la protection des données personnelles est modifiée comme il suit :

**Chapitre I But, champ d'application et définitions****Art. 3 Champ d'application**

<sup>1</sup> Sans changement.

<sup>2</sup> Sont soumises à la présente loi les entités suivantes :

- a. sans changement ;
- b. sans changement ;
- c. sans changement ;
- c<sup>bis</sup>. la Cour des comptes ;
- d. sans changement ;
- e. sans changement.

<sup>3</sup> La présente loi ne s'applique pas :

- a. sans changement ;
- b. sans changement ;
- c. aux données personnelles traitées en application de la loi fédérale sur le renseignement et de l'article 2, alinéa 1 de la loi sur les dossiers de police judiciaire.

**Chapitre II Dispositions générales***SECTION II TRAITEMENT DES DONNÉES PERSONNELLES***Art. 16 Procédure d'appel**

<sup>1</sup> Les données peuvent être rendues accessibles au moyen d'une procédure d'appel entre les entités soumise à la loi aux conditions de l'article 15. Les données sensibles ou les profils de la personnalité ne peuvent être rendus accessibles au moyen d'une procédure d'appel que si une loi au sens formel ou un règlement le prévoit.

<sup>2</sup> Sans changement.

**Chapitre III Fichiers****Art. 21a Exceptions**

<sup>1</sup> N'ont pas à être déclarés, s'ils ne contiennent pas de données sensibles ou ne constituent pas un profil de la personnalité :

- a. les fichiers renfermant uniquement des informations accessibles au public ;
- b. les fichiers d'enregistrement de la correspondance ;
- c. les fichiers d'adresses ;
- d. les fichiers éphémères dont la durée de vie n'excède pas un an.

**Chapitre IV Vidéosurveillance***SECTION I DISPOSITIONS GÉNÉRALES ET PROCÉDURE D'AUTORISATION***Art. 22 Principes**

<sup>1</sup> Les entités citées à l'article 3, alinéa 2 peuvent installer un système de vidéosurveillance dissuasive, avec ou sans système d'enregistrement, sur le domaine public ou leur patrimoine affecté à la réalisation d'une tâche publique, moyennant le respect des principes et prescriptions de la présente loi.

<sup>1bis</sup> Les buts d'un système de vidéosurveillance dissuasive sont de garantir la sécurité des personnes et des biens, d'éviter la perpétration d'infractions sur un certain lieu et de contribuer à la poursuite et à la répression d'infractions.

<sup>2</sup> Abrogé.

<sup>3</sup> Abrogé.

<sup>4</sup> Sans changement.

<sup>5</sup> Abrogé.

<sup>6</sup> Abrogé.

<sup>7</sup> Sans changement.

#### **Art. 22a Autorisation**

<sup>1</sup> Préalablement à son exploitation, l'installation de vidéosurveillance doit faire l'objet d'une demande d'autorisation du responsable du traitement. Il en va de même pour toute modification ultérieure du système.

<sup>2</sup> L'autorité compétente peut demander l'avis du Préposé avant de statuer. Le Préposé reçoit une copie de la décision.

<sup>3</sup> Si un système ne remplit plus les conditions légales, l'autorisation est retirée.

<sup>4</sup> Le Préposé publie une liste des installations de vidéosurveillance dissuasive qui ont été autorisées.

<sup>5</sup> Le Conseil d'Etat précise dans un règlement la procédure d'autorisation.

#### **Art. 22b Autorités compétentes**

<sup>1</sup> Lorsque la demande émane d'une entité cantonale, l'autorité compétente est le chef du département dont dépend l'entité concernée.

<sup>2</sup> Lorsque la demande émane d'une entité communale, l'autorité compétente est le préfet du district.

<sup>3</sup> Lorsque la demande émane d'un établissement de droit public cantonal ou d'une personne morale à laquelle le canton a confié des tâches publiques, l'autorité compétente est l'organe suprême de l'établissement.

#### **Art. 22c Recours**

<sup>1</sup> Le Préposé a la qualité pour recourir contre une décision d'autorisation auprès du Tribunal cantonal.

<sup>2</sup> Le responsable du traitement a la qualité pour recourir contre une décision de refus d'autorisation auprès du Tribunal cantonal.

#### **Art. 23a Durée de conservation des images**

<sup>1</sup> A moins qu'une autorité n'ordonne leur conservation dans le cadre d'une procédure pénale, les images enregistrées doivent être détruites automatiquement après un délai de sept jours, ou en cas d'atteinte aux personnes ou aux biens, après cent jours au maximum.

#### **Art. 23b Délégation**

<sup>1</sup> L'exploitation d'une installation de vidéosurveillance peut être déléguée à un tiers aux conditions de l'article 18.

<sup>2</sup> La délégation fait l'objet d'une décision d'autorisation en application de la procédure prévue aux articles 22a et 22b.

<sup>3</sup> Le responsable du traitement procède à des contrôles réguliers afin de s'assurer que les conditions légales sont respectées.

#### **Art. 23c Autorisation cadre**

<sup>1</sup> Si les besoins spécifiques d'une entité mentionnée à l'article 3, alinéa 2, lettres a à c<sup>bis</sup> le justifient, l'autorité compétente peut délivrer une autorisation de principe, dite autorisation cadre, permettant à l'entité bénéficiaire d'installer et d'exploiter, aux conditions définies par l'autorisation cadre, plusieurs installations de vidéosurveillance.

<sup>2</sup> Pour toute installation d'un système de vidéosurveillance, l'entité cantonale au bénéfice d'une autorisation cadre en informe l'autorité compétente et le Préposé.

<sup>3</sup> Le Conseil d'Etat précise dans un règlement les conditions d'octroi d'une autorisation cadre.

#### **Art. 23d Sécurité des données**

<sup>1</sup> Le responsable du traitement prend les mesures de sécurité appropriées afin de protéger les données enregistrées ou en transfert sur les réseaux informatiques et d'éviter tout traitement illicite de celles-ci. Il limite notamment l'accès aux données et aux locaux qui les contiennent.

<sup>2</sup> Il doit installer et maintenir un système de journalisation automatique permettant de contrôler les accès aux images.

#### **Art. 23e Traitement des données**

<sup>1</sup> L'accès aux images est limité aux personnes désignées par le responsable de traitement, ainsi qu'à celles qui peuvent se prévaloir d'un droit d'accès à leurs propres données, au sens du chapitre VI.

<sup>2</sup> Le responsable de traitement définit la procédure à suivre pour les opérations techniques de gestion des systèmes et des données informatiques liées à la vidéosurveillance.

<sup>3</sup> En vue d'obtenir des moyens de preuve, les images enregistrées peuvent être analysées en cas de dénonciation pénale, de plainte pénale ou d'indices concrets de la commission d'un acte pénalement punissable.

<sup>4</sup> Le responsable du traitement ne peut transmettre les images enregistrées qu'aux autorités chargées de poursuivre l'infraction pénale.

### *SECTION II DISPOSITIONS SPÉCIALES*

#### **Art. 23f Communes**

<sup>1</sup> Outre le respect des conditions posées à la section précédente, l'installation d'un système de vidéosurveillance sur le domaine public et le patrimoine affecté à la réalisation d'une tâche publique communale ou intercommunale nécessite l'adoption d'un règlement communal ou intercommunal.

<sup>2</sup> Les images enregistrées par le système de vidéosurveillance ne peuvent être utilisées que selon les modalités, aux conditions et aux fins fixées dans le règlement qui l'institue.

<sup>3</sup> Ce règlement ne peut déroger aux conditions minimales fixées par la loi.

#### **Art. 23g Etablissements scolaires**

<sup>1</sup> L'installation d'un système de vidéosurveillance dans ou aux abords immédiats d'un établissement scolaire communal ou intercommunal nécessite, outre l'autorisation prévue à l'article 22a, l'approbation du département chargé de la formation.

#### **Art. 23h Etablissements pénitentiaires**

<sup>1</sup> Les établissements pénitentiaires peuvent installer un système de vidéosurveillance de sécurité.

<sup>2</sup> Le Conseil d'Etat fixe les conditions à respecter quant à l'exploitation d'un système de vidéosurveillance de sécurité.

<sup>3</sup> Au surplus, les dispositions du présent chapitre ne s'appliquent pas à la vidéosurveillance dans les établissements pénitentiaires.

### **Chapitre VI Droits de la personne concernée**

#### **Art. 25 Droit d'accès à ses propres données**

<sup>1</sup> Sans changement.

<sup>2</sup> Sans changement.

<sup>3</sup> Sans changement.

<sup>4</sup> Sans changement.

#### **Art. 26a Délais**

<sup>1</sup> Le responsable de traitement répond dans les trente jours à compter de la date de réception de la demande par l'entité concernée.

### **Chapitre VII Procédure**

#### **Art. 32 b) Recours au Préposé et conciliation**

<sup>1</sup> Sans changement.

<sup>2</sup> Sans changement.

<sup>3</sup> Sans changement.

<sup>4</sup> Sans changement.

<sup>5</sup> Le responsable du traitement et l'intéressé peuvent recourir au Tribunal cantonal dans un délai de 30 jours dès la notification.

### **Chapitre VIII Préposé cantonal à la protection des données et à l'information**

#### **Art. 35 Statut et rattachement**

<sup>1</sup> Sans changement.

<sup>2</sup> Le Conseil d'Etat décide de son rattachement administratif.

<sup>3</sup> Sans changement.

#### **Art. 36 Tâches**

##### **1. Surveillance**

<sup>1</sup> Sans changement.

<sup>2</sup> Sans changement.

<sup>3</sup> Sans changement.

<sup>4</sup> L'entité concernée prend position par écrit. Si la recommandation du Préposé n'est pas suivie, ce dernier peut porter l'affaire devant le département ou l'entité concernée, pour décision.

<sup>5</sup> Le Préposé peut recourir contre la décision rendue conformément à l'alinéa précédent, ainsi que contre la décision rendue par l'autorité compétente (article 30). La loi sur la procédure administratives est applicable.

<sup>6</sup> Les rapports d'audit établis par le Préposé en application des dispositions qui précèdent sont communiqués au Président du Conseil d'Etat et au Président de la Commission de gestion du Grand Conseil.

##### **Art. 37 2. Autres tâches**

<sup>1</sup> Outre la surveillance mentionnée ci-dessus, le Préposé :

- a. sans changement ;
- b. sans changement ;
- c. sans changement ;
- d. sans changement ;
- e. sans changement ;
- f. peut être consulté sur les projets relatifs à l'installation de systèmes de vidéosurveillance et dispose en cette matière d'un droit de recours, conformément aux articles 22 et suivants de la présente loi ;
- g. sans changement ;
- h. sans changement.

<sup>2</sup> Sans changement.

#### **Art. 40 Rapport**

<sup>1</sup> Sans changement.

<sup>2</sup> Ce rapport est public. Il renseigne notamment sur les recommandations

prévues à l'article 36, alinéa 3 adressées dans l'année et, le cas échéant, sur les démarches entreprises par le Préposé en application de l'article 36, alinéas 4 et 5.

<sup>3</sup> Sans changement.

## **Chapitre IX Dispositions finales**

### **Art. 41 Violation du devoir de discrétion**

<sup>1</sup> Sans changement.

<sup>2</sup> Sans changement.

<sup>3</sup> Sans changement.

<sup>3bis</sup> Celui qui met en place une installation de vidéosurveillance sans en avoir au préalable demandé l'autorisation ou qui exploite une installation de vidéosurveillance sans en respecter les conditions légales sera puni de l'amende.

<sup>4</sup> Sans changement.

## **Chapitre X Dispositions transitoires et finales**

### **Art. 42 Application de la loi**

<sup>1</sup> Tout traitement des données doit se conformer à la présente loi, notamment en matière de légalité, dans les cinq ans suivant son entrée en vigueur.

<sup>2</sup> Abrogé.

<sup>3</sup> Tout système de vidéosurveillance dissuasive installé par les entités cantonales, les établissements de droit public, et les personnes morales auxquelles le canton a confié des tâches publiques, doit se conformer aux dispositions du chapitre IV de la présente loi dans un délai d'un an suivant l'entrée en vigueur de la loi du 5 juin 2018 modifiant la loi du 11 septembre 2007 sur la protection des données personnelles ; toutefois, les règles relatives à la durée de conservation des images sont immédiatement applicables.

<sup>4</sup> Toute modification d'un système de vidéosurveillance communal, autorisé avant l'entrée en vigueur de la loi du 5 juin 2018 modifiant la loi du 11 septembre 2007 sur la protection des données personnelles, est soumise à la procédure d'autorisation prévue au chapitre IV de la présente loi.

### **Art. 43**

<sup>1</sup> Abrogé.

<sup>2</sup> Abrogé.

### **Art. 2**

<sup>1</sup> Les demandes d'autorisations déposées avant l'entrée en vigueur de la loi du 5 juin 2018 modifiant la présente loi, et pour lesquelles une décision d'autorisation n'a pas encore été rendue, sont soumises à la procédure des articles 22 et suivants de la loi du 11 septembre 2007 sur la protection des données personnelles.

### **Art. 3**

<sup>1</sup> Le Conseil d'Etat est chargé de l'exécution de la présente loi. Il en publiera le texte conformément à l'article 84, alinéa 1, lettre a) de la Constitution cantonale et en fixera, par voie d'arrêté, la date d'entrée en vigueur.

Donné, sous le grand sceau de l'Etat, à Lausanne, le 5 juin 2018.

La présidente du Grand Conseil :                      Le secrétaire général du Grand  
Conseil :

*S. Podio*

*I. Santucci*

Le Conseil d'Etat ordonne la publication de la présente loi, conformément à l'article 84, alinéa 1, lettre a) de la Constitution cantonale.

Lausanne, le 13 juin 2018.

La présidente :

Le chancelier :

*N. Gorrite*

*V. Grandjean*

Date de publication : 19 juin 2018.

---

**ARRÊTÉ**  
**de mise en vigueur****170.50**du 5 septembre 2018

---

LE CONSEIL D'ÉTAT DU CANTON DE VAUD

vu le préavis du Service juridique et législatif

*arrête***Art. 1**

<sup>1</sup> Le décret du 5 juin 2018 sur la prévention de la radicalisation et de l'extrémisme violent (RSV 120.015), publié dans la "Feuille des avis officiels du Canton de Vaud" du 19 juin 2018, entre en vigueur le 5 juin 2018.

<sup>2</sup> La loi du 5 juin 2018 modifiant celle du 11 septembre 2007 sur la protection des données personnelles (RSVM 172.65), publiée dans la "Feuille des avis officiels du Canton de Vaud" du 19 juin 2018, entre en vigueur le 1er octobre 2018.

Donné, sous le sceau du Conseil d'Etat, à Lausanne, le 5 septembre 2018.

La présidente :

*N. Gorrite*

Le chancelier :

*V. Grandjean*