LOI 172.65
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 [A]

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

décrète

[A] *Constitution du Canton de Vaud du 14.04.2003 (BLV 101.01)*

Chapitre I But, champ d'application et définitions

Art. 1 But

[1] La présente loi vise à protéger les personnes contre l'utilisation abusive des données personnelles les concernant.

Art. 2 Terminologie

[1] La désignation des fonctions s'applique indifféremment aux femmes et aux hommes.

Art. 3 Champ d'application [4, 5, 6]

[1] La présente loi s'applique à tout traitement de données des personnes physiques ou morales.

[2] 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 ;

4 Modifié par la loi du 05.06.2018 entrée en vigueur le 01.10.2018
5 Modifié par la loi du 24.05.2022 entrée en vigueur le 01.01.2023
6 Modifié par la loi du 02.05.2023 entrée en vigueur le 01.09.2023

e. les personnes physiques et morales auxquelles le canton ou une commune confie des tâches publiques, dans l'exécution desdites tâches.

f. le Ministère public ;

g. le Conseil de la magistrature.

[3] 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.

Art. 4 Définitions

[1] 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

[1] 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.

[2] 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

[1] 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

[1] Le traitement des données personnelles doit être conforme au principe de la proportionnalité.

Art. 8 Transparence

[1] La collecte des données personnelles doit être reconnaissable pour la personne concernée.

Art. 9 Exactitude

[1] Les entités soumises à la présente loi s'assurent que les données personnelles traitées sont exactes.

Art. 10 Sécurité

[1] 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

[1] 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.

[2] 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

[1] 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

[1] Le responsable du traitement informe la personne concernée de toute collecte des données personnelles la concernant.

[2] 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.

[3] 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

[1] 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.

[2] 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

[1] 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.

[2] L'alinéa 1 est également applicable aux informations transmises sur demande en vertu de la loi sur l'information[B].

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

[B] Loi du 24.09.2002 sur l'information (BLV 170.21)

Art. 16 Procédure d'appel [4]

[1] 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.

[2] 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

[1] 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.

[2] 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

[1] 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.

---

[4] Modifié par la loi du 05.06.2018 entrée en vigueur le 01.10.2018

[2] Le tiers est responsable de la sécurité des données qu'il traite.

Chapitre III Fichiers

Art. 19 Registre des fichiers

[1] 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.

[2] Le Conseil d'Etat édicte les règles applicables à la tenue du registre [C] .

[C] Règlement du 29.10.2008 d'application de la loi du 11.09.2007 sur la protection des données personnelles (BLV 172.65.1)

Art. 20 Annonce

[1] 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.

[2] Le Conseil d'Etat fixe les renseignements à fournir lors de l'annonce de fichier.

Art. 21 Mise en service

[1] Les fichiers peuvent être opérationnels dès que le Préposé a été informé de leur constitution.

Art. 21a Exceptions [4]

[1] 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 [4]

Art. 22 Principes [4]

[1] 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.

---

[4] Modifié par la loi du 05.06.2018 entrée en vigueur le 01.10.2018

[1bis] 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.

[2] ...

[3] ...

[4] 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.

[5] ...

[6] ...

[7] Le Conseil d'Etat précise les conditions précitées.

Art. 22a Autorisation [4]

[1] 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.

[2] L'autorité compétente peut demander l'avis du Préposé avant de statuer. Le Préposé reçoit une copie de la décision.

[3] Si un système ne remplit plus les conditions légales, l'autorisation est retirée.

[4] Le Préposé publie une liste des installations de vidéosurveillance dissuasive qui ont été autorisées.

[5] Le Conseil d'Etat précise dans un règlement la procédure d'autorisation.

Art. 22b Autorités compétentes [4]

[1] Lorsque la demande émane d'une entité cantonale, l'autorité compétente est le chef du département dont dépend l'entité concernée.

[2] Lorsque la demande émane d'une entité communale, l'autorité compétente est le préfet du district.

[3] 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 [4]

[1] Le Préposé a la qualité pour recourir contre une décision d'autorisation auprès du Tribunal cantonal.

[2] Le responsable du traitement a la qualité pour recourir contre une décision de refus d'autorisation auprès du Tribunal cantonal.

---

[4] Modifié par la loi du 05.06.2018 entrée en vigueur le 01.10.2018

Art. 23 Indications

[1] Le responsable du traitement doit indiquer de manière visible l'existence du système de vidéosurveillance aux abords directs de ce dernier.

[2] Cette information inclut les coordonnées du responsable du traitement et mentionne le droit d'accès aux images concernées.

Art. 23a Durée de conservation des images [4]

[1] 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 [4]

[1] L'exploitation d'une installation de vidéosurveillance peut être déléguée à un tiers aux conditions de l'article 18.

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

[3] Le responsable du traitement procède à des contrôles réguliers afin de s'assurer que les conditions légales sont respectées.

Art. 23c Autorisation cadre [4]

[1] Si les besoins spécifiques d'une entité mentionnée à l'article 3, alinéa 2, lettres a à c[bis]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.

[2] 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.

[3] Le Conseil d'Etat précise dans un règlement les conditions d'octroi d'une autorisation cadre.

Art. 23d Sécurité des données [4]

[1] 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.

[2] Il doit installer et maintenir un système de journalisation automatique permettant de contrôler les accès aux images.

---

[4] Modifié par la loi du 05.06.2018 entrée en vigueur le 01.10.2018

Art. 23e Traitement des données [4]

[1] 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.

[2] 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.

[3] 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.

[4] Le responsable du traitement ne peut transmettre les images enregistrées qu'aux autorités chargées de poursuivre l'infraction pénale.

Section II Dispositions spéciales [4]

Art. 23f Communes [4]

[1] 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.

[2] 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.

[3] Ce règlement ne peut déroger aux conditions minimales fixées par la loi.

Art. 23g Etablissements scolaires [4]

[1] 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 [4]

[1] Les établissements pénitentiaires peuvent installer un système de vidéosurveillance de sécurité.

[2] Le Conseil d'Etat fixe les conditions à respecter quant à l'exploitation d'un système de vidéosurveillance de sécurité.

[3] Au surplus, les dispositions du présent chapitre ne s'appliquent pas à la vidéosurveillance dans les établissements pénitentiaires.

---

[4] Modifié par la loi du 05.06.2018 entrée en vigueur le 01.10.2018

Chapitre V Statistiques, planification et recherche

Art. 24

[1] 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.

[2] Les articles 5, 6, 15 de la présente loi ne sont pas applicables.

[3] La loi sur la statistique cantonale [D] est pour le surplus applicable.

[D] Loi du 15.09.1999 sur la statistique cantonale (BLV 431.01)

Chapitre VI Droits de la personne concernée

Art. 25 Droit d'accès à ses propres données [4]

[1] Toute personne a, en tout temps, libre accès aux données la concernant.

[2] Elle peut également requérir du responsable du traitement la confirmation qu'aucune donnée la concernant n'a été collectée.

[3] La personne qui fait valoir son droit doit justifier de son identité.

[4] Nul ne peut renoncer par avance au droit d'accès.

Art. 26 Modalités

[1] 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.

[2] La communication de données a lieu sur place ou se fait par écrit, sauf disposition contraire.

[3] Avec l'accord du requérant, la communication peut également se faire par oral.

[4] La communication des données est, en règle générale, gratuite.

[5] Le responsable du traitement qui répond à la demande peut percevoir un émolument :

a. lorsque la communication requiert un travail important ;

b. en cas de demandes répétitives ;

---

[4] Modifié par la loi du 05.06.2018 entrée en vigueur le 01.10.2018

c. lorsqu'une copie est demandée.

[6] Le Conseil d'Etat fixe le tarif des émoluments.

Art. 26a Délais [4]

[1] 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

[1] 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.

[2] Le droit d'accès aux données médicales est régi par la loi sur la santé publique [E] .

[3] Dès que le motif justifiant la restriction du devoir d'accès disparaît, le responsable du traitement doit fournir l'information.

[E] Loi du 29.05.1985 sur la santé publique (BLV 800.01)

Art. 28 Droit d'opposition

[1] 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.

[2] 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

[1] 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.

[2] Le cas échéant, elles peuvent demander au responsable du traitement de :

---

[4] Modifié par la loi du 05.06.2018 entrée en vigueur le 01.10.2018

a. rectifier, détruire les données ou les rendre anonymes ;

b. publier ou communiquer à des tiers la décision ou la rectification.

[3] 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

[1] 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.

[2] Le responsable du traitement adresse une copie de sa décision au Préposé.

Art. 31 Recours [3]

a) En général

[1] L'intéressé peut recourir au Préposé, ou directement au Tribunal cantonal.

[2] Au surplus, la loi sur la procédure administrative [F] est applicable aux décisions rendues en vertu de la présente loi, ainsi qu'aux recours contre dites décisions.

[F] *Loi du 28.10.2008 sur la procédure administrative (BLV 173.36)*

Art. 32 b) Recours au Préposé et conciliation [1, 2, 4]

[1] Dès qu'il est saisi du recours, le Préposé le notifie au responsable du traitement.

[2] 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.

[3] Si la conciliation aboutit, l'affaire est classée.

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

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

Art. 33 Gratuité [3]

[1] La procédure est gratuite.

[2] Un émolument peut être perçu en cas de demande abusive.

[3] ...

---

[3] Modifié par la loi du 28.10.2008 entrée en vigueur le 01.01.2009
[1] Modifié par le décret du 12.06.2007 entré en vigueur le 01.01.2008
[2] Modifié par le décret du 06.05.2008 entré en vigueur le 01.01.2009
[4] Modifié par la loi du 05.06.2018 entrée en vigueur le 01.10.2018

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

Art. 34 Désignation

[1] Le Préposé est désigné par le Conseil d'Etat, pour une période de 6 ans.

[2] Son mandat est renouvelable.

Art. 35 Statut et rattachement [4]

[1] Le Préposé exerce son activité de manière indépendante.

[2] Le Conseil d'Etat décide de son rattachement administratif.

[3] Le Préposé est tenu au secret de fonction.

Art. 36 Tâches [4]
1. Surveillance

[1] Le Préposé surveille l'application des prescriptions relatives à la protection des données.

[2] A cette fin, il dispose des moyens prévus à l'article 38 de la présente loi.

[3] 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.

[4] 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.

[5] 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[F] est applicable.

[6] 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.

[F] Loi du 28.10.2008 sur la procédure administrative (BLV 173.36)

Art. 37 2. Autres tâches [4]

[1] 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 ;

---

[4] Modifié par la loi du 05.06.2018 entrée en vigueur le 01.10.2018

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.

[2] En outre, le Préposé connaît des recours prévus à l'article 31 de la présente loi.

Art. 38 Moyens

[1] 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

[1] 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.

[2] Le secret de fonction ne peut être opposé au Préposé.

[3] Les tiers sont également tenus de fournir les renseignements requis par le Préposé.

Art. 40 Rapport [4]

[1] Le Préposé établit chaque année un rapport d'activité.

[2] 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.

[3] Le Préposé peut établir, en tout temps, un rapport spécial, d'office ou sur demande du Grand Conseil ou du Conseil d'Etat.

---

[4] Modifié par la loi du 05.06.2018 entrée en vigueur le 01.10.2018

Chapitre IX Dispositions finales [4]

Art. 41 Violation du devoir de discrétion [4]

[1] 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.

[2] 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.

[3] L'obligation de discrétion persiste au-delà de la fin des rapports de travail.

[3bis] 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.

[4] Le droit pénal fédéral est réservé.

Chapitre X Dispositions transitoires et finales

Art. 42 Application de la loi [4]

[1] 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] …

[3] 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.

[4] 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 … [4]

Art. 43a Dispositions transitoires de la loi du 05.06.2018 [G]

[1] 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.

---

[4] Modifié par la loi du 05.06.2018 entrée en vigueur le 01.10.2018

[G] *Correspond à l'article 2 de la loi modifiante du 05.06.2018*

Art. 44

[1] La loi du 25 mai 1981 sur les fichiers informatiques et la protection des données personnelles est abrogée.

Art. 45

[1] 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.