Entrée en vigueur dès le 01.09.2023 (Actuelle)

Document généré le : 26.02.2025

LOI 172.68
sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (LPrDS)

du 2 mai 2023

LE GRAND CONSEIL DU CANTON DE VAUD

en exécution de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

vu l'avant-projet de loi présenté par le Conseil d'Etat

décrète

Titre I Dispositions générales

Art. 1 Champ d'application

[1] La présente loi concerne la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales dans le cadre de l'application de l'acquis de Schengen et dans le cadre de l'application d'accords internationaux conclus avec l'Union européenne ou avec des Etats qui sont liés à la Suisse par l'un des accords d'association à Schengen (Etats Schengen).

[2] La présente loi ne s'applique pas aux droits des personnes concernées dans le cadre de procédures pendantes devant des tribunaux fédéraux ou cantonaux ou dans le cadre de procédures pendantes régies par le code de procédure pénale[A] ou par la loi du 20 mars 1981 sur l'entraide pénale internationale[B], ni dans le cadre de la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; ceux-ci sont régis par le droit de procédure applicable.

[A] Code de procédure pénale du 12.09.1967 (BLV 312.01)

[B] Loi fédérale du 20.03.1981 sur l'entraide internationale en matière pénale, RS 351.1

Art. 2 Définitions

[1] Par données génétiques, on entend les informations relatives au patrimoine génétique d'une personne obtenues par une analyse génétique, y compris le profil d'ADN.

[2] Par données biométriques, on entend les données personnelles résultant d'un traitement technique spécifique et relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique.

[3] Par profilage, on entend toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant la situation économique, la santé, les préférences personnelles, les intérêts, le comportement, la localisation ou les déplacements de cette personne.

[4] Par décision individuelle automatisée, on entend toute décision prise exclusivement sur la base d'un traitement de données personnelles automatisé, y compris le profilage, et qui a des effets juridiques sur la personne concernée ou qui l'affecte de manière significative.

[5] Les données génétiques ou biométriques sont des données sensibles au sens de la loi du 11 septembre 2007 sur la protection des données personnelles[C] (LPrD).

[6] Le Préposé, au sens de la présente loi est celui institué par la LPrD[C].

[7] Par violation de la sécurité des données, on entend toute violation de la sécurité, sans égard au fait qu'elle soit intentionnelle ou illicite, qui entraîne la perte de données personnelles, leur modification, leur effacement ou leur destruction, ou encore leur divulgation ou un accès non autorisés. La violation peut être causée par un tiers, mais son auteur peut aussi être un collaborateur qui outrepasse ses compétences ou qui fait preuve de négligence. La violation de la sécurité des données peut entraîner une perte de contrôle de la personne concernée sur ses données ou une utilisation abusive de celles-ci. Elle peut aussi engendrer une violation de la personnalité, par exemple en entraînant la divulgation d'informations que la personne souhaitait garder secrètes.

[C] Loi du 11.09.2007 sur la protection des données personnelles (BLV 172.65)

Titre II Obligations des organes traitant des données

Art. 3 Devoir d'informer la personne concernée en cas de décision individuelle automatisée

[1] Le responsable du traitement informe la personne concernée de toute décision individuelle automatisée prise à son égard, avant la prise de cette décision; il qualifie cette décision comme telle.

[2] Si la personne concernée le demande, le responsable du traitement lui donne la possibilité de faire valoir son point de vue. La personne concernée peut exiger que la procédure appliquée lui soit communiquée et que la décision soit revue par une personne physique.

[3] L'alinéa 2 du présent article ne s'applique pas lorsque la personne concernée dispose d'une voie de droit contre la décision.

Art. 4 Protection des données dès la conception et par défaut

[1] Les responsables du traitement sont tenus de mettre en place, dès la conception du traitement, des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données et en particulier les principes fixés par la présente loi.

[2] Les mesures techniques et organisationnelles doivent être appropriées au regard notamment de l'état de la technique, du type de traitement, de son étendue, ainsi que du risque que le traitement des données en question présente pour les droits fondamentaux des personnes concernées.

[3] Les responsables du traitement sont tenus, par le biais de préréglages appropriés, de garantir que le traitement soit limité au minimum requis par la finalité poursuivie.

Art. 5 Principe de légalité

[1] Une base légale formelle est nécessaire pour fonder un mode de traitement susceptible de porter atteinte aux droits fondamentaux ou un profilage.

[2] Une base légale formelle n'est pas nécessaire si :

a. il existe un besoin de protection de la vie ou de l'intégrité corporelle de la personne concernée ou d'un tiers, ou :

b. la personne concernée a rendu ses données personnelles accessibles à tout un chacun, ou :

c. la personne concernée ne s'est pas opposée expressément au traitement.

Art. 6 Registre des activités de traitement

[1] Les responsables du traitement tiennent un registre des activités de traitement.

[2] Les registres des responsables du traitement contiennent au moins les indications suivantes :

a. le nom du responsable du traitement;

b. la finalité du traitement;

c. une description des catégories des personnes concernées et des catégories des données personnelles traitées;

d. les catégories des destinataires;

e. la durée de conservation des données personnelles ou, si cela n'est pas possible, les critères pour déterminer la durée de conservation;

f. dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données;

g. l'Etat tiers ou l'organisme international auquel des données personnelles sont communiquées ainsi que les garanties de protection des données personnelles prévues.

Art. 7 Analyse d'impact relative à la protection des données personnelles

[1] Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour les droits fondamentaux de la personne concernée, Le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles. S'il envisage d'effectuer plusieurs opérations de traitements semblables, il peut établir une analyse d'impact commune.

[2] L'existence d'un risque élevé dépend, en particulier lors de l'utilisation de nouvelles technologies, de la nature, de l'étendue, des circonstances et de la finalité du traitement. Un tel risque existe notamment dans les cas suivants :

a. le traitement de données sensibles ou de profils de la personnalité à grande échelle;

b. le profilage.

[3] L'analyse d'impact contient une description du traitement envisagé, une évaluation des risques pour les droits fondamentaux de la personne concernée, ainsi que les mesures prévues pour protéger ceux-ci.

Art. 8 Consultation du Préposé

[1] Le responsable du traitement consulte le Préposé, préalablement au traitement, lorsque l'analyse d'impact relative à la protection des données révèle que le traitement présenterait un risque élevé pour les droits fondamentaux de la personne concernée si le responsable du traitement ne prenait pas de mesures pour atténuer ce risque.

[2] Le Préposé communique au responsable du traitement ses objections concernant le traitement envisagé dans un délai de deux mois. Ce délai peut être prolongé d'un mois, lorsqu'il s'agit d'un traitement de données complexe.

[3] Si le Préposé a des objections concernant le traitement envisagé, il propose au responsable du traitement des mesures appropriées.

Art. 9 Annonce des violations de la sécurité des données

[1] Le responsable du traitement annonce dans les meilleurs délais au Préposé les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour les droits fondamentaux de la personne concernée.

[2] L'annonce doit au moins indiquer la nature de la violation de la sécurité des données, ses conséquences et les mesures prises ou envisagées pour y remédier.

[3] Le sous-traitant annonce dans les meilleurs délais au responsable du traitement tout cas de violation de la sécurité des données.

[4] Le responsable du traitement informe la personne concernée lorsque cela est nécessaire pour sa protection ou lorsque le Préposé l'exige.

[5] Le responsable du traitement peut restreindre l'information de la personne concernée, la différer ou y renoncer, dans les cas suivants :

a. les intérêts prépondérants d'un tiers l'exigent;

b. un intérêt public prépondérant, en particulier le maintien de la sûreté intérieure ou extérieure du canton ou de la Suisse, l'exige;

c. l'information de la personne concernée est susceptible de compromettre une enquête, une instruction ou une procédure administrative ou judiciaire;

d. le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés;

e. l'information de la personne concernée est garantie de manière équivalente par une communication publique.

Art. 10 Conseiller à la protection des données

[1] Les responsables du traitement désignent un conseiller à la protection des données. Ils peuvent désigner un conseiller commun.

[2] Le conseiller à la protection des données doit remplir les conditions suivantes:

a. il dispose des connaissances professionnelles nécessaires;

b. il n'exerce pas d'activités incompatibles avec ses tâches de conseiller à la protection des données.

[3] Le conseiller à la protection des données exerce notamment les tâches suivantes :

a. il conseille les responsables du traitement;

b. il promeut l'information et la formation des collaborateurs;

c. il concourt à l'application des prescriptions relatives à la protection des données et propose des mesures s'il apparaît que des prescriptions relatives à la protection des données ont été violées.

Titre III Droits des personnes concernées

Art. 11 Prétentions et procédure

[1] Quiconque a un intérêt légitime peut exiger du responsable du traitement :

a. qu'il s'abstienne de procéder à un traitement illicite;

b. qu'il supprime les effets d'un traitement illicite;

c. qu'il constate le caractère illicite d'un traitement.

[2] Le demandeur peut en particulier exiger que le responsable du traitement :

a. rectifie les données personnelles, les efface ou les détruise;

b. publie ou communique à des tiers sa décision concernant notamment la rectification, l'effacement ou la destruction des données, l'opposition à une communication ou la mention du caractère litigieux des données personnelles prévue à l'alinéa 4 du présent article.

[3] Au lieu d'effacer ou de détruire les données personnelles, le responsable du traitement limite le traitement dans les cas suivants:

a. l'exactitude des données est contestée par la personne concernée et leur exactitude ou inexactitude ne peut pas être établie;

b. des intérêts prépondérants d'un tiers l'exigent;

c. un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure du canton ou de la Suisse, l'exige;

d. l'effacement ou la destruction des données est susceptible de compromettre une enquête, une instruction ou une procédure administrative ou judiciaire.

4 Si l'exactitude ou l'inexactitude d'une donnée personnelle ne peut pas être établie, il ajoute à la donnée la mention de son caractère litigieux.

5 La procédure est régie par la loi du 28 octobre 2008 sur la procédure administrative[D] (LPA).

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

Titre IV Surveillance

Art. 12 Enquête du Préposé

1 Le Préposé ouvre d'office ou sur dénonciation une enquête contre le responsable du traitement ou le sous-traitant si des indices font penser qu'un traitement de données personnelles pourrait être contraire à des dispositions de protection des données.

2 Il peut renoncer à ouvrir une enquête lorsque la violation des prescriptions de protection des données est de peu d'importance.

3 Le responsable du traitement ou le sous-traitant fournit au Préposé tous les renseignements et les documents qui lui sont nécessaires pour l'enquête.

4 Si la personne concernée est l'auteur de la dénonciation, le Préposé l'informe des suites données à celle-ci et du résultat d'une éventuelle enquête.

Art. 13 Pouvoirs du Préposé

1 Lorsque le responsable du traitement ou le sous-traitant ne respecte pas son obligation de collaborer, le Préposé peut, dans le cadre de la procédure d'enquête, ordonner notamment :

a. l'accès à tous les renseignements, documents, registres des activités et données personnelles nécessaires pour l'enquête;

b. l'accès aux locaux et aux installations;

c. l'audition de témoins;

d. des expertises.

2 Il peut également ordonner des mesures provisionnelles pour la durée de l'enquête.

Art. 14 Mesures administratives

[1] Si des dispositions de protection des données sont violées, le Préposé peut ordonner la mise en conformité, la suspension ou la cessation de tout ou partie du traitement ainsi que l'effacement ou la destruction de tout ou partie des données personnelles.

[2] Il peut suspendre ou interdire la communication de données personnelles à l'étranger si elle est contraire aux dispositions légales applicables en matière de communication de données personnelles à un Etat tiers ou à un organisme international.

[3] Lorsque le responsable du traitement ou le sous-traitant a pris, durant l'enquête, les mesures nécessaires au rétablissement d'une situation conforme aux prescriptions de protection des données, le Préposé peut se limiter à prononcer un avertissement.

[4] Les parties à la procédure d'enquête, y compris les responsables de traitement, ont qualité pour recourir, y compris contre les décisions sur l'effet suspensif ou les mesures provisionnelles.

Titre V Assistance administrative

Art. 15 Assistance administrative internationale

[1] Le Préposé peut échanger des informations ou des données personnelles avec une autorité d'un Etat Schengen chargée de la protection des données personnelles pour l'accomplissement de leurs tâches légales respectives en matière de protection des données, pour autant que les conditions suivantes soient réunies :

a. la réciprocité en matière d'assistance administrative est garantie;

b. les informations et les données personnelles échangées ne sont utilisées que dans le cadre de la procédure liée à la protection des données personnelles à la base de la demande d'assistance administrative;

c. l'autorité destinataire s'engage à ne pas divulguer les secrets professionnels, d'affaires ou de fabrication;

d. les informations et les données personnelles ne sont communiquées à des tiers qu'avec l'accord préalable de l'autorité qui les a transmises;

e. l'autorité destinataire s'engage à respecter les charges et les restrictions d'utilisation exigées par l'autorité qui lui a transmis les informations et les données personnelles.

[2] Pour motiver sa demande d'assistance administrative ou pour donner suite à une demande d'assistance administrative de l'autorité requérante, le Préposé peut communiquer notamment les indications suivantes :

a. le nom du service responsable du traitement, du sous-traitant ou de tout autre organe tiers participant au traitement;

b. les catégories de personnes concernées;

c. l'identité des personnes concernées lorsque sa communication est indispensable à l'accomplissement des tâches légales du Préposé ou d'une autorité d'un Etat Schengen chargée de la protection des données;

d. les données personnelles ou les catégories de données personnelles traitées;

e. les finalités des traitements;

f. les destinataires ou les catégories de destinataires;

g. les mesures techniques et organisationnelles.

[3] Avant de transmettre à une autorité d'un Etat Schengen chargée de la protection des données des informations susceptibles de contenir des secrets professionnels, de fabrication ou d'affaires, il informe les personnes détentrices de ces secrets et les invite à prendre position, à moins que cela ne s'avère impossible ou ne nécessite des efforts disproportionnés.

Titre VI Dispositions supplétives et transitoires

Art. 16 Dispositions supplétives

[1] A défaut de disposition spéciale prévue par la présente loi, la loi cantonale sur la protection des données personnelles[C] (LPrD) s'applique; l'applicabilité d'autres lois est réservée.

[2] La loi sur la procédure administrative[D] (LPA) s'applique en outre spécifiquement à la procédure à suivre concernant l'application des articles 11 à 14 de la présente loi.

[C] Loi du 11.09.2007 sur la protection des données personnelles (BLV 172.65)

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

Art. 17 Exécution et entrée en vigueur

[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, l'entrée en vigueur.