

PROJET DE LOI

sur la protection des données personnelles

LE GRAND CONSEIL DU CANTON DE VAUD

vu l'article 15 de la Constitution cantonale du 14 avril 2003

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

décète

Chapitre I But, champ d'application et organisation

Art. 1 But

¹ La présente loi vise à protéger les droits fondamentaux des personnes physiques ou morales dont les données personnelles font l'objet d'un traitement.

Art. 2 Champ d'application

¹ La présente loi régit le traitement de données personnelles de personnes physiques et morales par :

- a. les autorités cantonales au sens des articles 89 à 136d Cst-VD, leurs subdivisions et leurs administrations ;
- b. les communes et fractions de communes, les ententes intercommunales, associations et fédérations de communes, agglomérations et autres formes de collaborations intercommunales ;
- c. les autorités administratives indépendantes, cantonales ou communales, instituées par la loi ;
- d. les personnes morales de droit public ainsi que les autres entités autonomes, cantonales ou communales, créées par la loi ;
- e. les personnes physiques ou morales auxquelles les entités mentionnées aux lettres a à d confient une tâche publique, dans l'exécution de cette tâche ;
- f. les églises reconnues de droit public au sens de l'article 170 Cst-VD.

² Elle ne s'applique pas :

- a. aux délibérations du Grand Conseil et des conseils généraux et communaux ;
- b. aux procédures civiles, pénales, et administratives, à l'exception des procédures administratives de première instance ;
- c. sous réserve de l'alinéa 3, aux traitements de données personnelles réalisés par les entités mentionnées à l'alinéa 1 dans le cadre d'une activité soumise à la concurrence économique, régie par le droit privé. Ces traitements sont soumis aux dispositions de loi fédérale sur la protection des données régissant le traitement de données par des personnes privées, applicables par analogie.

³ La surveillance sur les traitements de données mentionnés à l'alinéa 2, lettre c, est exercée par l'Autorité de protection des données et de droit à l'information (ci-après : l'Autorité), selon les articles 40 à 43 de la présente loi.

Art. 3 Autorité de protection des données et de droit à l'information

¹ L'Autorité est dirigée par la Préposée cantonale ou le Préposé cantonal à la protection des données (ci-après : le Préposé). Elle est notamment chargée de surveiller la bonne application des dispositions cantonales en matière de protection des données personnelles et de droit à l'information.

² L'Autorité ne peut exercer aucune surveillance sur :

- a. le Grand Conseil ;
- b. le Conseil d'Etat ;
- c. le Tribunal cantonal.

³ Une Préposée ou un Préposé au droit à l'information représente l'Autorité dans l'accomplissement des tâches prévues à l'article 2b de la loi du 24 septembre 2002 sur l'information.

Art. 4 Personnes de référence en matière de protection des données

¹ Chaque département de l'Etat de Vaud désigne au minimum une personne spécialiste de la protection des données personnelles, disposant des connaissances professionnelles nécessaires, qui a pour tâches, au sein du département, de :

- a. conseiller les responsables du traitement ;
- b. informer les collaboratrices et collaborateurs ainsi que les responsables du traitement sur les exigences en matière de protection des données personnelles ;
- c. concourir à l'application des prescriptions relatives à la protection des données personnelles et proposer des mesures s'il apparaît que des prescriptions relatives à la protection des données personnelles ont été violées.

² Dans son domaine de compétence, le conseiller à la protection des données exécute les tâches mentionnées à l'alinéa 1 de manière indépendante par rapport au responsable du traitement et sans recevoir d'instruction de celui-ci. Il peut notamment contrôler les traitements de données personnelles et proposer des mesures correctives. Il fait en outre office de point de contact pour les personnes concernées et l'Autorité sur les questions relatives au traitement.

³ Dans les domaines qui relèvent de la directive (UE) 2016/680 relative à 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 (ci-après: directive Schengen), les responsables du traitement désignent un conseiller à la protection des données, disposant des connaissances professionnelles nécessaires et n'exerçant aucune activité incompatible avec sa mission. Ils veillent à ce que le conseiller à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données personnelles. Plusieurs responsables du traitement peuvent désigner un conseiller à la protection des données commun.

Chapitre II Dispositions générales, principes

Art. 5 Définitions

¹ On entend par :

- a. données personnelles : toutes les informations qui se rapportent à une personne physique ou morale identifiée ou identifiable ;
- b. données personnelles sensibles (ci-après : données sensibles) : les données personnelles :
 - 1. sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales ;
 - 2. sur la santé, l'origine ethnique ou la sphère intime d'une personne physique, en particulier sur son orientation sexuelle ;
 - 3. génétiques ;
 - 4. biométriques identifiant une personne physique de manière univoque ;
 - 5. sur les mesures d'aide sociale ;
 - 6. sur les poursuites ou sanctions pénales et administratives.
- c. profilage : toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique notamment afin d'analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne ;
- d. personne concernée : personne physique ou morale dont les données personnelles font l'objet d'un traitement ;
- e. traitement de données personnelles : toute opération relative à des données personnelles quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données ;
- f. communication : fait de rendre des données personnelles accessibles, notamment de les transmettre, les publier, autoriser leur consultation ou fournir des renseignements ;
- g. entité : toute personne, service et autorité visée à l'article 2 alinéa 1 ;
- h. responsable du traitement : l'entité qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles ;
- i. sous-traitant : toute personne physique ou morale, autorité publique ou tout autre organisme qui traite des données personnelles pour le compte du responsable du traitement ;
- j. violation de la sécurité des données : toute violation de la sécurité, sans égard au fait qu'elle soit accidentelle ou illicite, entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non-autorisé à ces données ;
- k. registre des activités de traitement : répertoire public inventoriant les activités de traitement réalisées par les responsables du traitement soumis à la présente loi ;

- I. 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.

Art. 6 Légalité

¹ Les données personnelles ne peuvent être traitées que si :

- a. une base légale l'autorise ; ou
- b. l'accomplissement d'une tâche légale l'exige.

² Les données sensibles ne peuvent être traitées, ou un profilage réalisé, que si :

- a. une loi au sens formel le prévoit expressément, ou
- b. l'accomplissement d'une tâche clairement définie dans une loi au sens formel l'exige absolument.

³ En dérogation aux alinéas 1 et 2, les entités désignées à l'article 2 alinéa 1 peuvent traiter des données personnelles, y compris des données sensibles, si une des conditions suivantes est remplie :

- a. le traitement est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et qu'il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable ;
- b. la personne concernée a consenti au traitement en l'espèce ou a rendu ses données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement ;
- c. le traitement des données personnelles est prévu dans le cadre d'essais pilotes au sens de l'article 23.

Art. 7 Finalité

¹ Les données personnelles 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.

² Elles ne peuvent être traitées ultérieurement que dans un but qui, selon les règles de la bonne foi, est compatible avec le but initial. Sont réservés les cas dans lesquels la personne concernée a consenti à un changement de finalité.

Art. 8 Proportionnalité

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

Art. 9 Transparence

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

Art. 10 Exactitude

¹ Le responsable du traitement s'assure que les données personnelles traitées sont exactes. Il prend toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Le caractère approprié de la mesure dépend notamment du type de traitement et de son étendue, ainsi que du risque que le traitement des données en question présente pour la personnalité ou les droits fondamentaux des personnes concernées.

Art. 11 Sécurité

¹ Le responsable du traitement et le sous-traitant doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru.

² Les mesures doivent permettre d'éviter toute violation de la sécurité des données.

³ Le Conseil d'Etat peut fixer des exigences minimales en la matière.

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 librement sa volonté concernant un ou plusieurs traitements déterminés, après avoir été dûment informée. Lorsqu'il s'agit de données sensibles ou de profilage, son consentement doit être au surplus exprès.

Art. 13 Protection des données dès la conception et par défaut

¹ Le responsable du traitement est tenu de mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données, en particulier les principes fixés aux articles 6 à 11. Il le fait dès la conception du traitement.

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 la personnalité et les droits fondamentaux des personnes concernées.

³ Le responsable du traitement est tenu de garantir, par le biais de prééglages appropriés, que le traitement des données personnelles soit limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement.

Chapitre III Traitement de données personnelles

Art. 14 Responsabilité

¹ Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont responsables conjoints du traitement et doivent définir de manière transparente leurs obligations respectives, à moins qu'elles ne résultent expressément d'une disposition légale.

Art. 15 Devoir d'informer lors de la collecte de données personnelles

¹ Le responsable du traitement informe la personne concernée de manière adéquate de la collecte de données personnelles, que celle-ci soit effectuée auprès d'elle ou non.

² Lors de la collecte, il communique à la personne concernée les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la présente loi et pour que la transparence des traitements soit garantie ; il lui communique au moins :

- a. l'identité et les coordonnées du responsable du traitement ;
- b. la finalité du traitement ;
- c. le cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises ;
- d. les catégories de données personnelles traitées.

³ Lorsque des données personnelles sont communiquées à l'étranger, il communique également à la personne concernée le nom de l'État ou de l'organisme international auquel elles sont communiquées et, le cas échéant, l'application d'une des exceptions prévues à l'article 20 alinéa 2.

⁴ Si les données personnelles ne sont pas collectées auprès de la personne concernée, il communique à cette personne les informations mentionnées à l'alinéa 2 au plus tard un mois après qu'il a obtenu les données personnelles. S'il communique les données personnelles avant l'échéance de ce délai, il en informe la personne concernée au plus tard lors de la communication.

Art. 16 Exceptions au devoir d'informer et restrictions

¹ Le responsable du traitement est délié du devoir d'information au sens de l'article 15 si l'une des conditions suivantes est remplie :

- a. la personne concernée dispose déjà des informations correspondantes ;
- b. le traitement des données personnelles ressort de la loi.

² Lorsque les données personnelles ne sont pas collectées auprès de la personne concernée, le devoir d'information ne s'applique pas non plus dans les cas suivants :

- a. l'information est impossible à donner ;
- b. elle nécessite des efforts disproportionnés.

³ Le responsable du traitement peut restreindre ou différer la communication des informations, ou y renoncer, si l'une des conditions suivantes est remplie :

- a. les intérêts prépondérants d'un tiers l'exigent ;
- b. l'information empêche le traitement d'atteindre son but ;
- c. un intérêt public prépondérant l'exige ;
- d. si la communication des informations est susceptible de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative.

Art. 17 Devoir d'informer en cas de décision individuelle automatisée

¹ Les décisions administratives qui sont rendues exclusivement sur la base d'un traitement de données personnelles automatisé doivent le mentionner.

² Le responsable du traitement doit garantir que le droit d'être entendu puisse être exercé préalablement au prononcé de la décision, lorsque la loi de procédure applicable l'exige.

³ La décision doit pouvoir être revue par une personne physique, dans le cadre d'une réclamation ou d'un recours.

Art. 18 Analyse d'impact

¹ Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou 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 traitement semblables, il peut établir une analyse d'impact commune.

² L'existence d'un risque élevé dépend 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 personnelles sensibles à grande échelle ;
- b. la surveillance systématique de grandes parties du domaine public.

³ L'analyse d'impact relative à la protection des données contient au moins :

- a. une description générale du traitement envisagé ;
- b. une évaluation des risques pour la personnalité ou les droits fondamentaux des personnes concernées ;
- c. les mesures prévues pour protéger la personnalité et les droits fondamentaux des personnes concernées.

⁴ Le responsable du traitement consulte l'Autorité préalablement au traitement lorsque l'analyse d'impact relative à la protection des données révèle que, malgré les mesures prévues par le responsable du traitement, le traitement envisagé présente encore un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

⁵ L'Autorité 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.

⁶ Si l'Autorité a des objections concernant le traitement envisagé, elle propose au responsable du traitement des mesures appropriées.

Art. 19 Communication de données personnelles

¹ Les entités soumises à la présente loi ne sont en droit de communiquer des données personnelles que dans les cas suivants :

- a. une base légale au sens de l'article 6 alinéa 1 lettre a, 6 alinéa 2 lettre a ou 6 alinéa 3 lettre c le prévoit ;

- b. lorsque les conditions d'application de l'article 6, alinéa 2, lettre b sont remplies, si une loi au sens matériel prévoit la communication de données et que cette communication ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée.

² En dérogation à l'alinéa 1, les entités soumises à la présente loi peuvent, dans un cas d'espèce, communiquer des données personnelles si l'une des conditions suivantes est remplie :

- a. la communication des données est indispensable à l'accomplissement d'une tâche légale du responsable du traitement ou du destinataire ;
- b. la personne concernée y a consenti ;
- c. la communication des données personnelles est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable ;
- d. la personne concernée a rendu ses données accessibles à tout un chacun et ne s'est pas expressément opposée à la communication ;
- e. le destinataire rend vraisemblable que la personne concernée ne refuse son consentement ou ne s'oppose à la communication que dans le but de l'empêcher de se prévaloir de prétentions juridiques ou de faire valoir d'autres intérêts légitimes ; à moins que cela ne s'avère impossible ou ne nécessite des efforts disproportionnés, la personne concernée sera auparavant invitée à se prononcer.

³ Les entités soumises à la présente loi peuvent en outre communiquer, spontanément ou sur demande des données personnelles dans le cadre de l'information au public, notamment en vertu de la loi sur l'information, à condition que la communication réponde à un intérêt public ou privé prévalant sur celui de la personne concernée.

Art. 20 Communication de données personnelles à l'étranger

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 exprès ;
- b. si la communication de données personnelles 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 et qu'il n'est pas possible d'obtenir son consentement dans un délai raisonnable ;

- f. si la communication provient 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, conventionnelles, techniques et organisationnelles, permettent d'assurer un niveau de protection adéquat à l'étranger. Le responsable du traitement informe l'Autorité des garanties applicables avant le traitement de données personnelles à l'étranger ;
- h. si un traité international garantit un niveau de protection approprié.

³ L'Autorité peut requérir du responsable du traitement qu'il fournisse des informations visant à vérifier qu'une communication de données personnelles à l'étranger répond aux exigences formulées aux lettres a à f.

⁴ Ne sont pas considérées comme faisant l'objet d'une communication de données personnelles à l'étranger les données qui sont publiées au moyen d'un site internet ouvert au public.

Art. 21 Traitement des données personnelles par un sous-traitant

¹ Le traitement de données personnelles peut être confié à un sous-traitant aux conditions cumulatives suivantes :

- a. le responsable du traitement serait en droit de réaliser lui-même le traitement de données concerné;
- b. le traitement par un sous-traitant est prévu par la loi ou par un contrat ;
- c. aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

² Le responsable du traitement demeure, à l'égard de la personne concernée, responsable de la sécurité des données personnelles traitées par le sous-traitant. Il doit en particulier s'assurer que le sous-traitant est en mesure de garantir la sécurité des données personnelles.

³ Le sous-traitant ne peut lui-même sous-traiter le traitement à un tiers qu'avec l'autorisation écrite préalable du responsable du traitement.

⁴ Lorsqu'une personne fait usage des droits prévus aux articles 26 à 31, le sous-traitant est tenu de fournir son assistance au responsable du traitement, dans la mesure nécessaire à traiter cette requête. Le responsable du traitement peut autoriser le sous-traitant à répondre directement à une demande d'accès aux données au sens de l'article 26.

Art. 22 Obligation d'annoncer les violations de la sécurité des données

¹ Le responsable du traitement annonce dans les meilleurs délais à l'Autorité, toute violation de la sécurité des données personnelles entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

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

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 à sa protection ou lorsque l'Autorité le demande.

⁵ Le responsable du traitement peut renoncer, en tout ou partie, à cette information ou l'ajourner dans les cas suivants :

- a. une loi au sens formel le prévoit expressément ;
- b. un intérêt public ou privé prépondérant l'exige ;
- c. le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés ;
- d. l'information de la personne concernée peut être garantie de manière équivalente par une communication publique.

Art. 23 Traitement de données personnelles dans le cadre d'essais pilotes

¹ Le Conseil d'Etat peut, dans le cadre d'un essai pilote, autoriser une entité cantonale, par voie d'arrêté, avant l'entrée en vigueur d'une loi au sens formel, à :

- a. traiter et communiquer des données sensibles ;
- b. réaliser des profilages.

² Un tel essai pilote ne peut être réalisé qu'en respect des conditions suivantes :

- a. les tâches que ce traitement permet d'accomplir sont prévues dans une loi au sens formel déjà en vigueur ;
- b. des mesures appropriées sont prises aux fins de réduire au minimum les atteintes aux droits fondamentaux de la personne concernée ;
- c. la mise en oeuvre du traitement rend indispensable une phase d'essai avant l'entrée en vigueur de la loi au sens formel, en particulier pour des raisons techniques.

³ L'Autorité est préalablement consultée. Sa prise de position est transmise au Conseil d'Etat.

⁴ Le responsable du traitement transmet, au plus tard deux ans après la mise en oeuvre de la phase d'essai, un rapport d'évaluation au Conseil d'Etat. Dans ce rapport, il lui propose la poursuite ou l'interruption du traitement. L'Autorité se détermine et sa prise de position figure au rapport.

⁵ Le traitement de données fondé sur un arrêté adopté en vertu de l'alinéa 1 doit être interrompu dans tous les cas si aucune base légale au sens de l'article 6 alinéa 2 n'est entrée en vigueur dans un délai de cinq ans à compter de la mise en oeuvre de l'essai pilote.

Art. 24 Conservation des données personnelles et proposition aux Archives cantonales

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 prévues par la loi cantonale sur l'archivage.

Art. 25 Statistiques, planification et recherche

¹ Les entités soumises à la présente loi sont en droit de traiter des données personnelles et de les communiquer à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la 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. les données sensibles ne sont communiquées à des personnes privées que sous une forme ne permettant pas d'identifier la personne concernée ;
- c. le destinataire ne communique les données personnelles à des tiers qu'avec le consentement de l'entité qui les lui a transmises ;
- d. les résultats du traitement sont publiés sous une forme ne permettant pas d'identifier la personne concernée.

² Les articles 6 alinéa 2, 7 et 19 de la présente loi ne sont pas applicables.

Chapitre IV Droits de la personne concernée

Art. 26 Droit d'accès à ses propres données

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

² Elle reçoit les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la présente loi et pour que la transparence du traitement soit garantie. Dans tous les cas, elle reçoit les informations suivantes :

- a. l'identité et les coordonnées du responsable du traitement ;
- b. les données personnelles traitées en tant que telles ;
- c. la finalité du traitement et, le cas échéant, la base légale du traitement ;
- d. la durée de conservation des données personnelles ou, si cela n'est pas possible, les critères pour fixer cette dernière ;
- e. les informations disponibles sur l'origine des données personnelles, dans la mesure où ces données n'ont pas été collectées auprès de la personne concernée ;
- f. le cas échéant, l'existence d'une décision individuelle automatisée ;
- g. le cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles sont communiquées, ainsi que les informations prévues à l'article 15 alinéa 3.

³ Elle peut également requérir du responsable du traitement la confirmation qu'aucune donnée la concernant n'a été collectée.

⁴ Le responsable du traitement qui fait traiter des données personnelles par un sous-traitant demeure tenu de fournir les renseignements demandés.

⁵ La personne qui fait valoir son droit doit justifier de son identité.

⁶ Nul ne peut renoncer par avance au droit d'accès.

Art. 27 Modalités

¹ La demande de droit d'accès n'est soumise à aucune exigence de forme. Elle doit toutefois contenir les indications suffisantes pour permettre d'identifier la donnée concernée.

² La personne qui fait valoir son droit d'accès a droit à une copie des données requises.

³ Avec l'accord du requérant, la communication peut se faire par oral ou sous un format électronique.

⁴ Le droit d'accès est, en règle générale, gratuit.

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

- a. lorsque la communication requiert un travail considérable ; ou
- b. en cas de demandes répétitives.

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

Art. 28 Délais

¹ Le responsable du traitement répond dans les trente jours à compter de la date de réception de la demande.

Art. 29 Restrictions

¹ Le responsable du traitement peut restreindre l'accès, voire refuser celui-ci, si :

- a. la loi le prévoit expressément ;
- b. un intérêt public ou privé prépondérant l'exige ;
- c. la demande d'accès est manifestement infondée notamment parce qu'elle poursuit un but contraire à la protection des données ou est manifestement procédurière.

² Dès que le motif justifiant la restriction du devoir d'accès disparaît, le responsable du traitement doit fournir l'information.

Art. 30 Droit d'opposition

¹ La personne concernée qui rend vraisemblable un intérêt digne de protection peut s'opposer à ce que le responsable du traitement communique des données personnelles déterminées.

² Le responsable du traitement rejette l'opposition si l'une des conditions suivantes est remplie:

- a. il est juridiquement tenu de communiquer les données personnelles;
- b. le défaut de communication risque de compromettre l'accomplissement de ses tâches.

Art. 31 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.

² Elles peuvent en particulier demander au responsable du traitement de :

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

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 V Autorité et Préposé

Art. 32 Désignation et statut

¹ Le Préposé est désigné par le Conseil d'Etat, pour une période de 5 ans.

² La période de fonction du Préposé peut être renouvelée une fois.

³ Le Préposé désigné est spécialisé dans le domaine de la protection des données et du droit à l'information.

⁴ La loi du 12 novembre 2001 sur le personnel de l'Etat de Vaud (LPers) s'applique aux rapports de travail du Préposé, sous réserve des dispositions particulières prévues par la présente loi.

Art. 33 Activités accessoires

¹ Le Préposé ne peut exercer aucune activité accessoire, lucrative ou non. Il ne peut pas non plus exercer une autre fonction au service de la Confédération, du canton ou d'une commune.

² Le Conseil d'Etat peut autoriser le Préposé à exercer une activité accessoire au sens de l'alinéa 1, pour autant que l'exercice de sa fonction, ainsi que l'indépendance et la réputation de l'Autorité n'en soient pas affectées. Sa décision est publiée.

Art. 34 Fin anticipée des rapports de travail

¹ Le Préposé peut résilier ses rapports de travail de manière anticipée, moyennant un préavis de six mois et pour la fin d'un mois.

² Le Conseil d'Etat peut révoquer le Préposé avant la fin de sa période de fonction:

- a. si le Préposé a gravement violé ses devoirs de fonction de manière intentionnelle ou par négligence grave;
- b. si le Préposé a durablement perdu la capacité d'exercer sa fonction.

³ La révocation prononcée selon l'alinéa 2 met fin aux rapports de travail avec le Préposé.

Art. 35 Collaborateurs de l'Autorité

¹ Le Préposé engage les collaborateurs de l'Autorité.

² La LPers s'applique aux rapports de travail des collaborateurs de l'Autorité.

Art. 36 Indépendance et organisation

¹ L'Autorité exerce son activité de manière indépendante et s'organise librement.

² L'Autorité dispose de son propre budget.

Art. 37 Rattachement

¹ L'Autorité est rattachée administrativement à la Chancellerie d'Etat.

Art. 38 Traitement des données par l'Autorité

¹ Pour accomplir les tâches qui lui incombent, l'Autorité peut traiter les données personnelles nécessaires à l'accomplissement de ses tâches, y compris des données sensibles.

² A cette fin, l'Autorité exploite un système de gestion électronique des dossiers.

³ Le règlement d'application de la présente loi fixe des dispositions d'exécution. Il définit en particulier :

- a. les catégories de données personnelles traitées ;
- b. les droits d'accès ;
- c. les mesures de sécurité techniques et organisationnelles destinées à empêcher le traitement des données par un tiers non-autorisé ;
- d. les délais de conservation des données ;
- e. l'archivage et l'effacement des données.

Art. 39 Autocontrôle de l'Autorité

¹ L'Autorité s'assure, par des mesures de contrôle appropriées portant notamment sur la sécurité des données personnelles, du respect et de la bonne application des dispositions cantonales de protection des données en son sein.

² L'Autorité décrit, dans son rapport d'activité annuel, les mesures d'autocontrôle qu'elle a réalisées durant l'année écoulée.

Chapitre VI Tâches et pouvoirs de l'Autorité

Art. 40 Enquête

¹ L'Autorité ouvre, d'office ou sur dénonciation, une enquête contre un responsable du traitement soumis à la présente loi, lorsque des indices suffisants font penser qu'un traitement de données personnelles pourrait être contraire à des dispositions de protection des données.

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

³ L'Autorité informe par écrit le responsable du traitement de l'ouverture d'une enquête, en précisant quels traitements de données personnelles sont visés.

⁴ Le responsable du traitement, ainsi que les tiers, fournissent à l'Autorité tous les renseignements et les documents qui lui sont nécessaires pour l'enquête. Le secret de fonction ne peut être opposé à l'Autorité, sous réserve du secret fiscal (article 157 LI). Pour le surplus, le droit de refuser de collaborer est régi par l'article 166 CPC.

⁵ Si la personne concernée est l'auteur de la dénonciation, l'Autorité peut l'informer des suites données à celle-ci et du résultat d'une éventuelle enquête.

⁶ Seul le responsable du traitement a la qualité de partie à la procédure d'enquête.

Art. 41 Pouvoirs

¹ Lorsque le responsable du traitement ou des tiers ne respectent pas leur obligation de collaborer, l'Autorité peut, dans le cadre de la procédure d'enquête, ordonner notamment :

- a. l'accès à tous les renseignements, documents, registres des activités de traitement et données personnelles nécessaires pour l'enquête ;
- b. l'accès aux locaux et aux installations ;
- c. l'audition de témoins ;
- d. des expertises.

² Dans le cadre des mesures d'instruction prévues à l'alinéa 1, le secret de fonction ne peut être opposé à l'Autorité, sous réserve du secret fiscal (article 157 LI). Pour le surplus, le droit de refuser de collaborer est régi par l'article 166 CPC.

³ Dans les domaines qui relèvent de la directive Schengen, l'Autorité peut également ordonner des mesures provisionnelles pour la durée de l'enquête.

Art. 42 Mesures administratives

¹ Si l'Autorité, après enquête, estime que des dispositions de protection des données sont violées, elle peut :

- a. ordonner d'informer les personnes concernées conformément aux articles 15 et 17 ;
- b. suspendre ou interdire la communication de données personnelles à l'étranger si elle est contraire aux conditions de l'article 20 ou à des dispositions d'autres lois fédérales concernant la communication de données personnelles à l'étranger.
- c. ordonner d'informer les personnes concernées conformément à l'article 22 ;
- d. ordonner d'annoncer le traitement au registre des activités de traitement conformément à l'article 48 ;
- e. ordonner la rectification, l'effacement ou la destruction de tout ou partie de certaines données personnelles ;

- f. impartir au responsable du traitement un délai approprié pour rétablir une situation conforme au droit ;
- g. à défaut d'exécution dans le délai fixé conformément à la lettre f, ordonner au responsable du traitement de suspendre ou cesser tout ou partie d'un traitement de données.

² Le responsable du traitement peut recourir au Tribunal cantonal contre la décision de l'Autorité dans les 30 jours dès sa notification.

³ Dans les domaines qui relèvent de la directive Schengen, l'Autorité peut également ordonner des mesures provisionnelles pour la durée de l'enquête.

Art. 43 Application de la procédure administrative vaudoise

¹ Au surplus, la loi du 28 octobre 2008 sur la procédure administrative (LPA-VD) s'applique à la procédure d'enquête et aux décisions rendues en application de l'article 42.

Art. 44 Autres tâches

¹ L'Autorité accomplit les autres tâches suivantes :

- a. elle promeut la protection des données personnelles dans le canton ;
- b. elle informe et conseille les responsables du traitement sur les exigences posées en matière de protection des données personnelles ;
- c. elle conseille les personnes concernées sur les droits découlant de la présente loi ;
- d. elle est consultée lors de l'élaboration de lois, règlements, directives ou autres normes impliquant le traitement de données personnelles ;
- e. elle tient à jour le Registre des activités de traitement institué à l'article 48 ;
- f. elle collabore avec les autres autorités compétentes en matière de protection des données des autres cantons, de la Confédération ou de l'étranger.

Art. 45 Coopération avec d'autres autorités de protection des données en Suisse

¹ Dans l'exercice de ses tâches, l'Autorité coopère avec les autorités fédérales, cantonales et communales chargées de la protection des données.

² Dans ce cadre, l'Autorité communique, spontanément ou sur demande, aux autorités chargées de la protection des données les informations ou les données personnelles, y compris les données sensibles, nécessaires à l'accomplissement de leurs tâches légales respectives.

Art. 46 Coopération avec d'autres autorités de protection des données à l'étranger

¹ Dans l'exercice de ses tâches, l'Autorité coopère avec les autorités étrangères chargées de la protection des données.

² Dans ce cadre, l'Autorité peut, spontanément ou sur demande, communiquer des informations ou des données personnelles, y compris des données sensibles, à des autorités étrangères chargées de la protection des données, pour autant que cela soit nécessaire à l'accomplissement de leurs tâches légales respectives et 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 qui a donné lieu à 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.

³ Avant de transmettre à une autorité étrangère des informations susceptibles de contenir des secrets professionnels, de fabrication ou d'affaires, l'Autorité informe les personnes physiques ou morales détentrices de ces secrets et les invite à prendre position, à moins que cela ne s'avère impossible ou ne nécessite des efforts disproportionnés.

Art. 47 Audit

¹ L'Autorité peut réaliser des audits des responsables du traitement soumis à la présente loi afin de les sensibiliser aux exigences de protection des données personnelles et de leur proposer des améliorations.

² L'Autorité détermine l'étendue de l'audit et la communique au responsable du traitement concerné.

³ L'Autorité peut confier la réalisation de l'audit à un tiers prestataire.

⁴ Les rapports d'audit établis en application des dispositions qui précèdent sont communiqués à l'entité concernée, à sa hiérarchie, à la Présidence du Conseil d'Etat et à la Présidence de la Commission de gestion du Grand Conseil. Pour le surplus, ces rapports ne sont pas publics.

Art. 48 Rapport annuel

¹ L'Autorité établit chaque année un rapport d'activité.

² Elle présente son rapport au Conseil d'Etat et au Grand Conseil en mai de chaque année.

³ Le rapport d'activité est public.

⁴ En sus du rapport d'activité, l'Autorité peut, s'il en va de l'intérêt général, informer le public de ses constatations et de ses décisions.

Chapitre VII Registre des activités de traitement

Art. 49 Registre des activités de traitement

¹ L'Autorité tient un registre des activités de traitement qui est public.

² Il contient pour chaque activité de traitement des informations sur :

- a. l'identité et les coordonnées du responsable du traitement ;

- b. la base légale du traitement ;
- c. les finalités du traitement ;
- d. les personnes concernées ou les catégories de personnes concernées ;
- e. les données personnelles ou les catégories de données personnelles traitées ;
- f. les destinataires ou les catégories de destinataires des données personnelles si la communication des données personnelles est envisagée, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- g. la durée de conservation ou, si cela n'est pas possible, les critères pour déterminer cette durée ;
- h. dans la mesure du possible, les mesures visant à garantir la sécurité des données personnelles.

³ Le Conseil d'Etat édicte les règles applicables à la tenue du registre.

Art. 50 Annonce

¹ Les entités soumises à la présente loi sont tenues d'annoncer sans délai à l'Autorité leurs activités de traitement.

Art. 51 Exceptions

¹ Dans la mesure où ils sont exécutés exclusivement à des fins administratives internes propres à une entité publique déterminée, les traitements suivants ne sont pas soumis à l'obligation de déclarer :

- a. les annuaires publics de données personnelles ;
- b. l'enregistrement et la gestion de la correspondance ;
- c. la tenue de listes d'adresses ;
- d. la gestion et la tenue des documents qui ont été déposés aux archives historiques ;
- e. les activités de traitement concernant des fins ne se rapportant pas aux personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique.

Chapitre VIII Voies de droit, procédure

Art. 52 Décision du responsable du traitement

¹ Lorsqu'il refuse une demande fondée sur les articles 26 à 31, le responsable du traitement rend une décision comprenant les motifs l'ayant conduit à ne pas y donner suite.

² Si la personne concernée le sollicite, le responsable du traitement adresse une copie de cette décision à l'Autorité, pour information.

Art. 53 Recours

¹ Le recours contre la décision rendue en application de l'article 52 est régi par la LPA-VD.

² Les procédures de première instance et de recours sont gratuites. Un émolument peut néanmoins être perçu en cas d'abus.

Chapitre IX Dispositions pénales

Art. 54 Violation du devoir de discrétion

¹ Toute personne ayant révélé intentionnellement, d'une manière illicite, des données personnelles ou sensibles qui ont été portées à sa connaissance en qualité de délégataire de tâches légales, 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.

Art. 55 Dénonciation par l'Autorité

¹ L'Autorité peut dénoncer des infractions aux autorités de poursuite pénale compétentes.

Chapitre X Dispositions transitoire et finales

Art. 56 Abrogation

¹ La loi du 11 septembre 2007 sur la protection des données personnelles (LPrD) est abrogée.

² La loi du 2 mai 2023 sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (LPrDS) est abrogée.

Art. 57 Dispositions transitoires

¹ Les entités désignées à l'article 2, alinéa 1 qui, au jour de l'entrée en vigueur de la présente loi, traitent des données génétiques ou biométriques, ou réalisent des profilages, sur la base de dispositions conformes à l'ancienne LPrD, ont un délai d'un an pour adapter leurs législations.

² Les entités désignées à l'article 2, alinéa 1 ont un délai de cinq ans pour renseigner le nouveau registre des activités de traitement.

³ Les procédures de recours prévues par la présente loi ne s'appliquent pas aux recours déposés avant son entrée en vigueur, sur la base de l'ancienne LPrD ou de la LPrDS. Dans ces affaires, l'ancien droit s'applique.

⁴ Le Préposé en poste au jour de l'entrée en vigueur de la présente loi reste en fonction jusqu'au terme du mandat de 6 ans prévu par l'article 34, alinéa 1 de l'ancienne LPrD.

Art. 58 Disposition finale

¹ Le Conseil d'Etat est chargé de l'exécution de la présente loi qui est sujette au référendum facultatif.

² Il en publiera le texte et en fixera, par voie d'arrêté, la date d'entrée en vigueur.