

Loi sur la protection des données (LPrD)

du ...

Actes concernés (numéros RSF):

Nouveau: **17.1**

Modifié(s): 110.1 | 122.0.1 | 130.1 | 140.1 | 150.1 | 17.3 | 17.5 | 181.1 |
184.1 | 411.0.1 | 412.0.1 | 610.1 | 821.0.1

Abrogé(s): 17.1

Le Grand Conseil du canton de Fribourg

Vu l'article 12 al. 1 de la Constitution du canton de Fribourg du 16 mai 2004 (Cst.);

Vu le message 2023-CE-149 du Conseil d'Etat du 26 juin 2023;

Sur la proposition de cette autorité,

Décrète:

I.

1 Dispositions générales

Art. 1 But

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

Art. 2 Champ d'application personnel

¹ La loi s'applique aux organes publics suivants:

- a) les organes de l'Etat, des communes et les autres personnes morales de droit public;
- b) les personnes privées et les organes d'institutions privées lorsqu'ils accomplissent des tâches de droit public.

² Elle s'applique aux Eglises reconnues à moins qu'elles aient adopté des dispositions en matière de protection des données garantissant un niveau de protection adéquat et qu'elles aient institué leur propre autorité de surveillance.

Art. 3 Champ d'application matériel

¹ La présente loi s'applique à tous les traitements de données personnelles accomplis par un organe public au sens de l'article 2.

² Font exception:

- a) les traitements de données effectués dans le cadre de procédures civiles, pénales et de juridiction administrative en cours;
- b) les traitements de données qui servent à l'usage exclusivement personnel de celui ou de celle qui les effectue;
- c) les traitements de données accomplis par un organe public en situation de concurrence économique avec des personnes de droit privé.

Art. 4 Définitions

¹ On entend par:

- a) données personnelles: toutes les informations qui se rapportent à une personne identifiée ou identifiable;
- b) personne concernée: la personne physique ou morale au sujet de laquelle des données sont traitées;
- c) données personnelles sensibles (données sensibles):
 - 1. les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales;
 - 2. les données sur la santé, la sphère intime ou l'origine raciale ou ethnique;
 - 3. les données génétiques;
 - 4. les données biométriques identifiant une personne physique de manière univoque;
 - 5. les données sur des mesures d'aide sociale;
 - 6. les données sur des poursuites ou des sanctions pénales et administratives.
- d) traitement: toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, l'enregistrement, la conservation, l'exploitation, la modification, la communication, l'interconnexion, l'externalisation, l'effacement, l'archivage ou la destruction;

- e) procédure d'appel: le mode de communication automatisé des données par lequel les destinataires, en vertu d'une autorisation du responsable du traitement, décident de leur propre chef, sans contrôle préalable, du moment et de l'étendue de la communication;
- f) profilage: toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne, notamment pour 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;
- g) externalisation: une forme qualifiée de sous-traitance impliquant l'utilisation de ressources informatiques accessibles à distance, via un réseau de communication, pour stocker, traiter et partager des données (informatique en nuage);
- h) responsable du traitement: l'organe public qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles;
- i) sous-traitant: la personne privée ou l'organe public qui traite des données personnelles pour le compte du responsable du traitement;
- j) registre des activités de traitement: répertoire en ligne inventoriant les activités de traitement réalisées par les organes publics;
- k) violation de la sécurité des données personnelles: toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données.

2 Principes régissant le traitement de données personnelles

2.1 Conditions générales de licéité du traitement

Art. 5 Base légale

¹ L'organe public n'est en droit de traiter des données personnelles que si une disposition légale le prévoit ou si l'accomplissement d'une tâche légale l'exige.

² Le traitement de données sensibles ne peut avoir lieu 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 et la finalité du traitement ne présente pas de risques particuliers pour les droits fondamentaux des personnes concernées.

³ Les activités de profilage et les traitements de données personnelles, dont les finalités ou les modalités présentent un risque élevé pour les droits fondamentaux des personnes concernées, ne peuvent avoir lieu que si une loi au sens formel le prévoit expressément.

⁴ Exceptionnellement, une base légale n'est pas exigée pour traiter des données personnelles, y compris sensibles, lorsque le traitement est nécessaire pour sauvegarder les intérêts essentiels de la personne concernée ou d'un tiers.

Art. 6 Consentement

¹ En dehors des cas prévus à l'article 5, la personne concernée peut, dans un cas d'espèce, consentir au traitement de ses données personnelles.

² La personne concernée ne consent valablement que si elle exprime sa volonté librement et après avoir été dûment informée sur les finalités du traitement. Le consentement doit être exprès lorsqu'il porte sur un traitement de données sensibles ou sur des activités de profilage. Toutefois, le consentement est présumé lorsque la personne a elle-même rendu ses données librement accessibles.

³ Tout traitement de données qui ne repose pas sur l'un des fondements prévus à l'article 5 doit s'accompagner d'une mention visible et facilement compréhensible de son caractère facultatif.

⁴ Lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement doit être en mesure de démontrer l'existence d'un tel consentement.

⁵ Le consentement peut être révoqué en tout temps et sans motif. La mise en œuvre effective du retrait du consentement peut toutefois requérir un délai raisonnable pour des raisons techniques.

Art. 7 Finalité

¹ Les données personnelles ne peuvent être collectées que pour un usage déterminé et reconnaissable. Elles ne peuvent être traitées ultérieurement que dans ce but ou dans un but qui, selon les règles de la bonne foi, est compatible avec lui.

² Sont réservés les cas dans lesquels la personne concernée a consenti à un changement de finalité.

Art. 8 Proportionnalité

¹ Les données et les modes de traitement doivent être nécessaires, appropriés et non excessifs par rapport au but du traitement.

Art. 9 Exactitude

¹ L'organe public qui traite des données personnelles veille à leur exactitude. Il prend toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard de la finalité de leur traitement.

Art. 10 Délai de conservation

¹ Les données personnelles qui ne sont plus nécessaires au regard des finalités du traitement sont détruites ou anonymisées. Sont réservées les dispositions en matière d'archivage.

² Moyennant des mesures de protection appropriées, des données peuvent être conservées pour des durées plus longues dans la mesure où, conformément à l'article 26, elles servent exclusivement à des fins ne se rapportant pas à la personne.

Art. 11 Devoir de diligence accru

¹ L'organe public qui traite des données sensibles, exerce des activités de profilage ou traite des données pour des finalités ou selon des modalités présentant un risque accru d'atteinte aux droits fondamentaux doit prendre toutes les dispositions nécessaires pour diminuer les risques.

2.2 Conditions supplémentaires applicables à certaines formes de traitement

Art. 12 Collecte – Devoir d'informer

¹ Le responsable du traitement informe la personne concernée de manière adéquate de la collecte de données personnelles.

² Lorsque la collecte de données personnelles s'effectue directement auprès de la personne concernée, le responsable du traitement veille à lui fournir au moins les informations suivantes:

- a) le responsable du traitement et ses coordonnées;
- b) la finalité du traitement;
- c) cas échéant, les destinataires ou les catégories de destinataires auxquels les données personnelles sont transmises;
- d) le caractère obligatoire ou facultatif de la collecte des données.

³ Si les données personnelles sont collectées auprès d'un autre organe ou de tiers, le responsable du traitement communique à la personne concernée, dans les meilleurs délais mais au plus tard lors de leur première utilisation, les informations mentionnées à l'alinéa 1, ainsi que le type de données collectées.

Art. 13 Collecte – Exceptions au devoir d'informer

¹ Le responsable de traitement est délié de son devoir d'information dans les cas suivants:

- a) lorsque la personne concernée dispose déjà des informations correspondantes;
- b) lorsqu'il est impossible d'informer la personne concernée ou que cela impliquerait des efforts disproportionnés;
- c) lorsque la collecte résulte d'une obligation légale à moins qu'elle ne soit réalisée directement auprès de la personne concernée.

² Il peut en outre être dérogé au devoir d'informer aux mêmes conditions et pour les mêmes motifs que ceux indiqués à l'article 29 al. 1.

Art. 14 Communication – Conditions

¹ Des données personnelles ne peuvent être communiquées, transmises, diffusées ou rendues accessibles de manière systématique que si une disposition légale le prévoit.

² Des données personnelles peuvent être communiquées dans un cas d'espèce si:

- a) la communication est indispensable à l'accomplissement des tâches légales du responsable du traitement ou du ou de la destinataire des données;
- b) la personne concernée a consenti à la communication;
- c) la personne privée qui demande les données justifie d'un intérêt à la communication primant celui de la personne concernée à ce que les données ne soient pas communiquées.

³ Dans le cas prévu à l'alinéa 2 let. c, la personne concernée sera préalablement invitée à se prononcer à moins que cela ne s'avère impossible ou ne nécessite des efforts disproportionnés.

⁴ L'accès à des données personnelles au moyen d'une procédure d'appel, notamment un accès en ligne, ne peut être accordé que si une disposition légale le prévoit.

Art. 15 Communication – Conditions supplémentaires pour les communications transfrontières

¹ Les données personnelles d'une personne physique peuvent être communiquées vers un Etat étranger ou vers un organisme international dans la mesure où il existe une décision du Conseil fédéral attestant que l'Etat ou l'organisme international destinataire des données garantit un niveau de protection adéquat.

² En l'absence d'une telle décision, la communication ne peut avoir lieu que si:

- a) des garanties suffisantes, notamment contractuelles, conventionnelles, techniques et/ou organisationnelles, permettent d'assurer un niveau de protection adéquat à l'étranger;
- b) la communication est, en l'espèce, indispensable soit à la sauvegarde d'un intérêt public prépondérant, soit à la constatation, l'exercice ou la défense d'un droit en justice;
- c) la personne concernée a, en l'espèce, donné son consentement explicite à la communication;
- d) le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat, et les données traitées concernent une partie au contrat;
- e) la communication est, en l'espèce, nécessaire à la protection de la vie ou de l'intégrité corporelle de la personne concernée ou d'un tiers.

³ Avant la communication des données personnelles à l'étranger, le ou la préposé-e à la transparence et à la protection des données (ci-après: le ou la préposé-e) est informé-e à temps des garanties prévues à l'alinéa 2 let. a. Sur demande, il ou elle peut en tout temps obtenir des informations visant à vérifier qu'une communication de données à l'étranger répond aux exigences formulées aux lettres b à e.

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

Art. 16 Communication – Restrictions

¹ La communication est refusée, restreinte ou assortie de charges:

- a) si un intérêt public prépondérant ou un intérêt digne de protection de la personne concernée ou d'un tiers le commande, ou
- b) si une obligation légale de garder le secret ou une disposition particulière de protection des données l'exige.

Art. 17 Communication – Réserves

¹ La communication des données personnelles qui sont inscrites au contrôle des habitants et dans le Référentiel cantonal est régie par les lois y relatives.

² La communication de données personnelles au public est régie par la législation sur l'information et l'accès aux documents.

Art. 18 Externalisation – Principes

¹ Le traitement de données personnelles, y compris de données sensibles, peut être externalisé aux conditions posées par la présente loi.

² Les lieux de traitement doivent être situés en tout temps sur le territoire suisse ou sur le territoire d'un Etat garantissant un niveau de protection des données adéquat.

³ Lorsque l'externalisation implique une délégation de tâches à des tiers au sens de l'article 54 Cst., les exigences particulières prévues par cette disposition sont applicables.

⁴ Le Conseil d'Etat présente tous les deux ans à la Commission des finances et de gestion un rapport sur l'externalisation.

Art. 19 Externalisation – Responsabilités

¹ L'organe public qui procède à une externalisation demeure responsable de la protection des données personnelles, en particulier de leur confidentialité ainsi que de la pérennité de leur conservation et de leur exploitation. En particulier:

- a) il prend les précautions commandées par les circonstances quant au choix du sous-traitant, à son instruction et à sa surveillance;
- b) il assure la protection et la sécurité des données et de ses propres systèmes d'information par la conclusion d'un contrat qui décrit au minimum:
 1. l'objet, la nature, la finalité et la durée de l'externalisation;
 2. les catégories de données concernées;
 3. les obligations et les droits de chaque partie;
 4. les droits et les possibilités de contrôle sur le sous-traitant;
 5. l'interdiction faite au sous-traitant de sous-traiter à son tour un traitement sans l'autorisation préalable du responsable du traitement;
 6. le devoir du sous-traitant d'informer immédiatement le responsable du traitement lorsque, en vertu d'une loi étrangère ou d'une décision de justice, il est tenu de communiquer des données à une autorité étrangère ou risque de devoir le faire.
- c) il ne confie pas au sous-traitant des traitements qu'il ne serait pas en droit d'effectuer lui-même;
- d) il veille à ce que les données concernées par une externalisation puissent être récupérées en temps utile, notamment dans le but de changer de sous-traitant, de procéder à leur réinternalisation ou de les verser aux archives historiques;
- e) il rend le sous-traitant attentif à ses obligations en matière de confidentialité, notamment au regard du secret de fonction et/ou du secret professionnel.

² Au sein de l'administration cantonale, la responsabilité de la mise en œuvre et du suivi des règles en matière d'externalisation est assumée conjointement par l'organe compétent à raison de la matière et par le service en charge de l'informatique ¹⁾. Sont réservés les cas dans lesquels l'organe compétent à raison de la matière gère de manière autonome tout ou partie de ses systèmes informatiques.

³ Lorsque l'externalisation concerne plusieurs organes différents au sein d'une même collectivité publique, un organe principalement responsable est désigné. L'alinéa 2 s'applique pour le surplus.

Art. 20 Externalisation – Mesures de sécurité

¹ L'intégrité, l'authenticité, la disponibilité et la confidentialité des données personnelles externalisées ainsi que la pérennité de leur conservation et de leur exploitation doivent être garanties par des mesures organisationnelles et techniques appropriées et adaptées à l'évolution des technologies disponibles.

² La définition des mesures de sécurité tient compte des risques que le traitement des données en question présente pour les droits fondamentaux des personnes concernées.

³ Lorsque l'externalisation concerne des données indispensables au fonctionnement de l'administration, la continuité des activités externalisées doit, en cas d'incident, être garantie par un dispositif adéquat.

Art. 21 Externalisation – Mesures relatives aux données sensibles

¹ Le traitement de données personnelles sensibles et le traitement de données qui font l'objet d'une obligation légale ou contractuelle de garder le secret peuvent être externalisés si la confidentialité à l'égard du sous-traitant est assurée de manière que ce dernier ne puisse avoir accès à leur contenu.

² Lorsque le sous-traitant doit impérativement avoir accès aux données pour des raisons techniques, le contrat d'externalisation fixe les exigences particulières nécessaires, en particulier l'engagement du sous-traitant de n'accéder au contenu des données qu'avec le consentement exprès de l'organe public qui procède à l'externalisation et l'obligation de tenir un journal des accès.

³ Lors de l'externalisation de données soumises à une obligation légale de garder le secret, le responsable du traitement s'assure que le sous-traitant ait le statut d'auxiliaire du détenteur du secret.

¹⁾ Actuellement: Service de l'informatique et des télécommunications.

Art. 22 Projets pilotes incluant le traitement de certaines catégories de données

¹ Lorsqu'un projet pilote au sens de l'article 35 de la loi du 18 décembre 2020 sur la cyberadministration (LCyb) inclut le traitement de données sensibles ou d'autres types de traitement au sens de l'article 5 al. 3, l'organe responsable du projet pilote:

- a) transmet le dossier prévu à l'article 35 al. 2 let. d LCyb à l'Autorité cantonale de la transparence, de la protection des données et de la médiation (ci-après: l'Autorité de surveillance) au plus tard un mois avant sa transmission au Conseil d'Etat;
- b) transmet le rapport d'évaluation au sens de l'article 35a al. 2 LCyb à l'Autorité de surveillance au plus tard un mois avant sa transmission au Conseil d'Etat;
- c) prend les mesures nécessaires afin d'assurer la protection des droits fondamentaux et des données personnelles des personnes concernées durant tout le déroulement du projet pilote.

² Le dossier du projet pilote et le rapport d'évaluation doivent contenir chacun au minimum une partie consacrée au traitement des données personnelles ainsi qu'à leur protection.

³ L'Autorité de surveillance peut prendre position sur le contenu du dossier du projet pilote et du rapport d'évaluation. Sa prise de position est communiquée au Conseil d'Etat.

Art. 23 Archivage

¹ Les données personnelles sont soumises à la législation sur l'archivage; leur valeur archivistique est déterminée en collaboration avec les organes en charge des archives historiques.

Art. 24 Effacement et destruction

¹ Les données personnelles dont la conservation ne poursuit plus aucune finalité et qui n'ont pas de valeur archivistique sont effacées ou détruites dès que possible par des moyens appropriés qui assurent leur élimination sécurisée.

² Les supports de données sont détruits au moment de leur recyclage ou de leur remplacement lorsqu'il existe un risque que des données sensibles ayant été effacées puissent être consultées par des personnes non autorisées.

Art. 25 Vidéosurveillance

¹ Les règles en matière de vidéosurveillance sont énoncées dans la législation y relative.

2.3 Traitements de données à des fins ne se rapportant pas à la personne

Art. 26 Règles

¹ Les organes publics sont en droit de traiter des données personnelles et de les communiquer à des fins ne se rapportant pas à la personne – notamment dans le cadre de la recherche, de la planification ou de la statistique – aux conditions suivantes:

- a) les données sont détruites ou rendues anonymes dès que la finalité du traitement le permet;
- b) le ou la destinataire ne communique les données à des tiers qu'avec le consentement de la personne ou de l'organe qui les lui a transmises;
- c) les données sensibles ne sont transmises à des personnes privées que sous une forme ne permettant pas d'identifier les personnes concernées;
- d) les résultats du traitement sont publiés sous une forme ne permettant pas d'identifier les personnes concernées.

² Les articles 5 al. 2 et 3, 7 et 14 al. 1 ne sont pas applicables.

³ Les personnes privées qui reçoivent des données personnelles de la part d'un organe public en vue d'un traitement à des fins ne se rapportant pas à la personne s'engagent par écrit à prendre toutes les précautions nécessaires pour protéger la personnalité des personnes concernées.

3 Droits de la personne concernée

Art. 27 Droit d'accès – Principes

¹ Toute personne peut demander au responsable du traitement si des données personnelles la concernant sont traitées.

² Le droit d'accès porte en particulier sur les informations suivantes:

- a) le responsable du traitement et ses coordonnées;
- b) les données personnelles traitées;
- c) la finalité et, le cas échéant, les bases juridiques du traitement;
- d) le délai de conservation des données personnelles ou, si cela n'est pas possible, les critères pour fixer ce dernier;
- e) les informations disponibles sur l'origine des données personnelles;
- f) le cas échéant, la logique et les critères d'une mesure ou d'une décision prise sur la base d'un traitement automatisé de données;

g) le cas échéant, les destinataires ou les catégories de destinataires auxquels des données ont été ou seront communiquées, ainsi que les informations prévues à l'article 15 al. 3.

³ L'organe public qui fait traiter des données par un sous-traitant demeure tenu de communiquer les données et de fournir les renseignements demandés.

⁴ Nul ne peut renoncer par avance à son droit d'accès.

Art. 28 Droit d'accès – Modalités

¹ La personne qui fait valoir son droit d'accès doit justifier de son identité.

² Les renseignements sont, en règle générale, fournis par écrit sur un support physique ou de façon électronique. En accord avec le responsable du traitement, la personne concernée peut également consulter ses données sur place.

³ La procédure est gratuite. Le Conseil d'Etat peut prévoir des exceptions.

Art. 29 Droit d'accès – Restrictions

¹ Le responsable du traitement peut refuser, restreindre ou différer la communication des données si et dans la mesure où :

- a) une loi au sens formel le prévoit;
- b) un intérêt public prépondérant le commande, notamment si la communication des renseignements risque de compromettre une procédure ou une enquête en cours;
- c) l'intérêt prépondérant d'un tiers le commande;
- d) la demande d'accès est manifestement abusive, notamment en raison de son caractère répétitif.

² La communication des données versées aux archives historiques peut également être refusée, restreinte ou différée lorsque le traitement de la demande est incompatible avec une gestion administrative rationnelle et que la personne concernée ne fait pas valoir un intérêt digne de protection à son exécution.

³ Le responsable du traitement doit indiquer pour quel motif il refuse, restreint ou diffère la communication des renseignements.

Art. 30 Données des personnes décédées

¹ Sur demande, le responsable du traitement accorde la consultation gratuite des données personnelles d'une personne décédée si :

- a) la personne demanderesse a un intérêt à obtenir ces renseignements, et
- b) aucun intérêt public ou privé prépondérant, notamment celui de la personne décédée ou de ses proches, ne s'y oppose.

² Un intérêt à la consultation des données est établi en présence d'un lien de parenté proche, d'un mariage ou d'une communauté de vie analogue au mariage avec la personne décédée.

³ Pour l'accès aux données soumises au secret professionnel, l'article 321 du code pénal suisse est réservé.

Art. 31 Opposition à la communication de données personnelles

¹ La personne concernée peut s'opposer par avance à ce que le responsable du traitement communique des données personnelles déterminées.

² Malgré l'opposition de la personne concernée, la communication peut néanmoins avoir lieu lorsque:

- a) elle est prévue par la loi;
- b) le défaut de communication risque de compromettre l'accomplissement de tâches de l'organe public;
- c) la personne qui requiert les données est une personne privée et les deux conditions ci-après sont remplies:
 1. il n'existe aucun obstacle juridique à la communication;
 2. le requérant ou la requérante rend vraisemblable que la personne concernée 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.

³ Dans les situations visées à l'alinéa 2 let. c, la personne concernée sera préalablement entendue dans la mesure du possible. Le responsable du traitement statue sur la communication au moyen d'une décision.

⁴ Les articles 11 et 27 al. 1 let. c et al. 2 de la loi du 9 septembre 2009 sur l'information et l'accès aux documents (LInf) sont réservés.

Art. 32 Portabilité des données

¹ La personne concernée peut demander au responsable du traitement qu'il lui remette sous un format électronique couramment utilisé les données personnelles la concernant lorsque les conditions suivantes sont réunies:

- a) le responsable du traitement traite les données personnelles de manière automatisée, et
- b) la législation spéciale prévoit expressément l'existence d'un droit à la portabilité ou le responsable du traitement a, de son propre chef, décidé d'introduire une telle possibilité.

² Pour autant que les conditions de l'alinéa 1 soient remplies et que cela n'exige pas des efforts disproportionnés, la personne concernée peut en outre demander au responsable du traitement qu'il transmette les données personnelles la concernant à un autre responsable du traitement.

³ Le responsable du traitement remet ou transmet gratuitement les données personnelles. La législation spéciale est réservée.

Art. 33 Actions défensives

¹ Quiconque a un intérêt digne de protection peut exiger du responsable du traitement qu'il:

- a) s'abstienne de procéder à un traitement illicite;
- b) mette un terme à un traitement illicite;
- c) constate le caractère illicite d'un traitement.

² En particulier, il ou elle peut demander au responsable du traitement qu'il:

- a) rectifie les données inexacts le ou la concernant ou supprime les données dont la conservation ne poursuit plus aucune finalité;
- b) limite temporairement le traitement de certaines données déterminées le ou la concernant, notamment leur modification ou leur communication à des tiers;
- c) fasse figurer une mention appropriée à propos de données le ou la concernant dont ni l'exactitude ni l'inexactitude ne peuvent être prouvées;
- d) publie une décision qui le ou la concerne ou la communique à des tiers.

³ Les données personnelles contenues dans des fonds d'archive ou des fonds ouverts au public ne peuvent être ni rectifiées ni détruites. La personne concernée ou toute personne qui dispose d'un intérêt digne de protection peut cependant demander que l'institution limite l'accès aux données litigieuses et/ou insère au dossier l'inscription d'une mention appropriée.

Art. 34 Procédure et voies de droit

¹ Le code de procédure et de juridiction administrative est applicable aux décisions prises en application de la présente section. Ces décisions sont sujettes à recours.

² A moins que la personne concernée ne s'y oppose, l'organe qui a rendu une décision au sens de l'alinéa 1 la communique à l'Autorité de surveillance.

³ L'Autorité de surveillance a qualité pour recourir contre la décision.

Art. 35 Réparation du dommage et du tort moral

¹ La personne qui subit un préjudice en raison d'une violation des dispositions de la présente loi peut faire valoir des prétentions en dommages-intérêts et en réparation du tort moral conformément à la loi sur la responsabilité civile des collectivités publiques et de leurs agents.

² Elle peut demander que le ou la juge ordonne la publication ou la communication à des tiers de tout ou partie de son jugement.

4 Mise en œuvre de la protection des données

Art. 36 Responsabilité – En général

¹ Tout organe public qui traite des données personnelles est responsable de la protection des données.

² Lorsque plusieurs organes publics traitent conjointement des données, la répartition de leurs obligations relatives à la protection des données est réglée dans la déclaration prévue à l'article 38, à moins qu'elle ne résulte expressément d'une disposition légale.

³ La répartition des responsabilités établie conformément à l'alinéa 2 n'est pas opposable à la personne concernée.

Art. 37 Responsabilité – Sous-traitance

¹ L'organe public qui fait traiter des données personnelles par un sous-traitant demeure responsable des obligations prévues par la législation en matière de protection des données.

² Le traitement de données personnelles peut être confié à un sous-traitant pour autant qu'un contrat ou une convention le prévoit et que les conditions suivantes soient réunies:

- a) seuls sont effectués les traitements que le responsable du traitement serait en droit d'effectuer lui-même;
- b) aucune obligation légale ou contractuelle de garder le secret ne l'interdit;
- c) le sous-traitant n'est pas autorisé à confier à son tour le traitement à un tiers sans l'autorisation préalable du responsable du traitement.

³ Le responsable du traitement doit en particulier s'assurer que le sous-traitant est en mesure de garantir la sécurité des données.

⁴ Le sous-traitant peut faire valoir les mêmes motifs justificatifs que le responsable du traitement.

⁵ A moins que la loi ou une convention entre organes n'en dispose autrement, les règles en matière de sous-traitance ne s'appliquent pas entre organes appartenant à une même collectivité. L'article 36 al. 2 est applicable.

Art. 38 Registre des activités de traitement – Principes

¹ L'Autorité de surveillance tient un registre public des activités de traitement de l'administration cantonale, des communes et, sauf si elles ont fait usage de la possibilité prévue à l'article 2 al. 1 let. c, des Eglises reconnues.

² Pour chaque activité de traitement, ce registre contient les informations suivantes:

- a) le responsable du traitement auprès duquel les personnes concernées peuvent faire valoir leurs droits à titre principal et ses coordonnées;
- b) le cas échéant, les autres responsables du traitement, leurs coordonnées et la répartition des responsabilités;
- c) le cas échéant, les sous-traitants et leurs coordonnées;
- d) la dénomination, la base légale et la finalité du traitement;
- e) une description des catégories de personnes concernées et des catégories de données personnelles traitées;
- f) les destinataires réguliers de données.

³ Chaque responsable du traitement déclare à l'Autorité de surveillance les activités de traitement qu'il accomplit et leurs modifications successives.

⁴ En cas de traitements conjoints de données, le responsable du traitement qui remplit la déclaration du traitement adresse une copie de cette dernière aux autres responsables du traitement.

Art. 39 Registre des activités de traitement – Exceptions

¹ Dans la mesure où ils sont exécutés exclusivement à des fins administratives internes propres à un organe public déterminé, 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 tenue de listes de fournisseurs et fournisseuses et de clients et clientes;
- e) la tenue et la gestion des pièces comptables lorsqu'elles contiennent des données personnelles;
- f) la gestion et la tenue des documents qui ont été déposés aux archives historiques;
- g) 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.

² Sur préavis de l'Autorité de surveillance, le Conseil d'Etat peut prévoir des exceptions à l'obligation de déclarer pour d'autres catégories de traitements qui ne présentent manifestement pas de risques pour les droits des personnes concernées.

Art. 40 Mesures organisationnelles et techniques

¹ Le responsable du traitement est tenu de mettre en place des mesures techniques et organisationnelles appropriées afin que le traitement respecte la présente loi, en particulier les principes énoncés à la section 2.1. Il le fait dès la conception du traitement.

² Les mesures mises en place sont harmonisées avec celles visant à assurer la sécurité des informations de l'administration en général, ainsi qu'avec les mesures de sécurité informatique.

³ Le responsable du traitement est tenu de garantir, par le biais de préréglages appropriés, que le traitement est limité au minimum requis par la finalité poursuivie.

⁴ Les mesures mises en place et le choix des réglages sont documentés.

Art. 41 Analyse d'impact – Principes

¹ Lorsqu'un nouveau traitement de données est susceptible d'engendrer un risque élevé pour les droits fondamentaux de la personne concernée, le responsable du traitement procède préalablement à une analyse d'impact relative à la protection des données personnelles.

² L'existence d'un risque élevé dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Présentent notamment un risque élevé:

- a) les traitements de données sensibles à grande échelle;
- b) les activités de profilage;
- c) la surveillance systématique de grandes parties du domaine public;
- d) les traitements d'une ampleur ou d'une intensité particulière recourant à des technologies, à des mécanismes ou à des procédures accentuant le risque d'atteinte aux droits fondamentaux des personnes concernées.

³ L'analyse d'impact contient une description du traitement envisagé, une évaluation des risques du point de vue technique et juridique ainsi qu'une description des mesures prévues pour protéger les droits fondamentaux des personnes concernées.

Art. 42 Analyse d'impact – Consultation de l'Autorité de surveillance

¹ Le responsable du traitement consulte l'Autorité de surveillance lorsque le résultat de l'analyse d'impact confirme l'existence d'un risque élevé pour les droits fondamentaux des personnes concernées nécessitant de prendre des mesures de précaution particulières.

² L'Autorité de surveillance communique ses éventuelles objections et recommandations concernant le traitement envisagé dans un délai de deux mois. Exceptionnellement, ce délai peut être prolongé d'un mois, lorsqu'il s'agit d'un traitement de données complexe.

³ Le responsable du traitement informe l'Autorité de surveillance de la suite donnée au plus tard au moment de débiter le traitement ayant fait l'objet de l'analyse d'impact.

Art. 43 Violations de la sécurité des données – Mesures à prendre

¹ Lorsqu'il constate une violation de la sécurité des données personnelles, le responsable du traitement prend immédiatement les mesures appropriées afin de mettre fin à la violation et d'en minimiser les effets.

² Il consigne dans un document interne la nature de la violation, le type de données concernées et les catégories de personnes touchées, les conséquences probables pour ces dernières et les mesures prises pour y remédier.

³ Le responsable du traitement annonce dans les plus brefs délais au ou à la préposé-e les cas de violation de la sécurité des données personnelles entraînant vraisemblablement un risque élevé pour les droits fondamentaux de la personne concernée.

⁴ Le responsable du traitement fait en sorte que le sous-traitant lui annonce sans tarder toute violation de la sécurité des données personnelles survenue chez lui.

Art. 44 Violations de la sécurité des données – Annonce à la personne concernée

¹ Lorsque cette mesure s'impose pour des motifs de transparence et/ou pour permettre à la personne concernée de prendre les mesures utiles à la sauvegarde de ses intérêts, le responsable du traitement informe cette dernière de la survenance d'une violation de la sécurité des données.

² Exceptionnellement, il 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 l'exige, en particulier la sécurité intérieure ou l'ordre public;

- c) l'information est susceptible de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative en cours;
- d) le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés.

³ Lorsque la violation de la sécurité des données touche un grand nombre de personnes, l'information peut avoir lieu sous la forme d'une communication publique. Le responsable du traitement veille dans ce cas à fournir une information aussi complète que possible.

Art. 45 Correspondants et correspondantes en matière de protection des données

¹ Chaque Direction désigne au minimum un correspondant ou une correspondante à la protection des données. Cette fonction peut être cumulée avec d'autres fonctions, notamment dans le domaine de la sécurité de l'information.

² Le correspondant ou la correspondante à la protection des données exerce notamment les tâches suivantes:

- a) il ou elle sensibilise les responsables de traitements au domaine de la protection des données;
- b) il ou elle conseille et assiste les responsables de traitements sur demande de ceux-ci ou si une affaire l'exige;
- c) il ou elle participe avec le responsable du traitement à la réalisation des analyses d'impact relatives à la protection des données prévues à l'article 41;
- d) il ou elle est l'interlocuteur ou l'interlocutrice privilégié-e de l'Autorité de surveillance pour toutes les questions de protection des données;
- e) il ou elle accomplit toutes les autres tâches que la loi lui confie.

³ Le correspondant ou la correspondante à la protection des données exerce ses fonctions de manière autonome. Les responsables du traitement lui communiquent d'office ou sur demande toutes les informations utiles à l'accomplissement de ses tâches.

⁴ Les correspondants et les correspondantes à la protection des données forment entre eux un réseau de compétence. Le Conseil d'Etat règle l'organisation et le fonctionnement du réseau.

⁵ Le Conseil d'Etat peut étendre l'obligation de désigner un correspondant ou une correspondante à la protection des données à d'autres entités de l'administration cantonale que les Directions.

5 Surveillance

Art. 46 En général

¹ La surveillance de la protection des données à l'échelle du canton et des communes est assurée par l'Autorité cantonale de la transparence, de la protection des données et de la médiation (en abrégé: l'Autorité de surveillance).

5.1 Autorité de surveillance

Art. 47 Organisation

¹ L'Autorité de surveillance comprend la Commission cantonale de la transparence, de la protection des données et de la médiation (ci-après: la Commission), le ou la préposé-e à la transparence et à la protection des données (en abrégé: le ou la préposé-e) et le médiateur ou la médiatrice cantonal-e.

² Elle exerce les tâches qui lui incombent en vertu de la présente loi par l'intermédiaire de la Commission et du ou de la préposé-e.

³ Les tâches qu'elle exerce dans les domaines du droit d'accès aux documents et de la médiation administrative sont régies par les législations y relatives.

Art. 48 Statut

¹ L'Autorité de surveillance est indépendante dans l'exercice de ses fonctions.

² Elle est rattachée administrativement à la Direction dont elle relève. Elle a son propre secrétariat et dispose des ressources nécessaires à l'accomplissement effectif de ses fonctions et à l'exercice de ses pouvoirs.

³ L'Autorité dispose d'une enveloppe budgétaire dont le montant est déterminé chaque année à l'occasion de l'adoption du budget de l'Etat. Elle adresse auparavant sa propre proposition de budget au Conseil d'Etat. Cette proposition est traitée conformément à l'article 61 al. 1 let. a de la loi du 16 octobre 2001 sur l'organisation du Conseil d'Etat et de l'administration.

⁴ Les membres de l'Autorité de même que ses collaborateurs et collaboratrices sont soumis au secret de fonction et à l'obligation de discrétion.

⁵ Au moment de leur entrée en fonction et lors de chaque changement de situation, les membres de l'Autorité signalent les liens particuliers qui les rattachent à des intérêts privés ou publics. L'article 14 al. 1 let. b et al. 2 et 3 LInf s'appliquent par analogie.

⁶ Les articles 21 à 25 du code de procédure et de juridiction administrative du 23 mai 1991 sont applicables à la récusation des membres de l'Autorité.

Art. 49 Commission – Composition et organisation

¹ La Commission cantonale de la transparence, de la protection des données et de la médiation est formée d'un président ou d'une présidente et de six membres, élus par le Grand Conseil à la suite d'une proposition du Conseil d'Etat.

² Le président ou la présidente et les membres doivent posséder, dans leur ensemble, les connaissances nécessaires à l'accomplissement des tâches de la Commission; celle-ci comprend, en particulier, un ou une juriste, un ou une professionnel-le de la santé, un ou une spécialiste en informatique et en sécurité des données et un ou une professionnel-le des médias.

³ Le secrétariat de la Commission est assuré par le ou la préposé-e; pour les dossiers en lien avec les activités de médiation, le secrétariat peut être assuré par le médiateur ou la médiatrice cantonal-e.

⁴ En cas de besoin, la Commission peut consulter des experts ou des expertes et inviter des tierces personnes à assister à tout ou partie de ses séances et, le cas échéant, à s'y exprimer avec voix consultative.

⁵ Pour le surplus, la Commission règle son organisation et son fonctionnement.

Art. 50 Commission – Attributions

¹ La Commission exerce une surveillance générale dans le domaine de la protection des données. Elle a notamment pour attributions:

- a) de mener en collaboration avec la Direction à laquelle elle est rattaché la procédure de nomination du ou de la préposé-e pour le Conseil d'Etat et de préavisier à son intention la ou les candidatures privilégiées;
- b) de diriger l'activité du ou de la préposé-e;
- c) de donner son avis sur les projets d'actes législatifs touchant à la protection des données ainsi que dans les cas prévus par la loi;
- d) de donner son avis sur les projets pilotes menés conformément à l'article 22;
- e) d'interjeter les recours prévus à l'article 34 al. 3;
- f) de prononcer des décisions en matière de protection des données conformément à l'article 58;
- g) de veiller à la coordination entre les exigences de la protection des données et l'exercice du droit d'accès aux documents officiels.

² La Commission adresse chaque année au Grand Conseil, par l'intermédiaire du Conseil d'Etat, un rapport sur son activité ainsi que sur celle du ou de la préposé-e et du médiateur ou de la médiatrice cantonal-e. Dans la mesure où l'intérêt général le justifie, elle peut informer le public de ses constatations.

Art. 51 Préposé-e – Nomination et statut

¹ Le ou la préposé-e à la transparence et à la protection des données est nommé-e pour une période individuelle de 5 ans par le Conseil d'Etat. Cet engagement est reconductible.

² Durant toute la durée de son engagement, le ou la préposé-e ne peut exercer aucune activité susceptible de porter atteinte à l'indépendance de sa fonction ou qui serait d'une autre manière incompatible avec les tâches de l'Autorité de surveillance. L'exercice d'une charge publique accessoire ou d'une activité lucrative accessoire est soumis à autorisation de la Commission.

³ Au moment de son engagement et durant toute la durée de ses rapports de service, le ou la préposé-e doit posséder les qualifications et/ou l'expérience nécessaires à l'exercice de ses fonctions.

⁴ Pour autant que la présente loi ou son ordonnance d'exécution n'en dispose pas autrement, les rapports de fonction du ou de la préposé-e sont régis par la législation sur le personnel de l'Etat. Son évaluation annuelle au sens de cette législation est réalisée par la Commission.

Art. 52 Préposé-e – Reconduction et fins des rapports de fonction

¹ La période de fonction du ou de la préposé-e est reconduite tacitement. Toutefois, le Conseil d'Etat peut, au plus tard six mois avant l'échéance de la période de fonction, rendre une décision de non-reconduction. Il demande à cet effet le préavis de la Commission. Cette décision doit être fondée sur de justes motifs.

² Moyennant un préavis de trois mois, le ou la préposé-e peut demander au Conseil d'Etat de mettre fin à la période de fonction pour la fin d'un mois.

³ Le ou la préposé-e peut être révoqué-e de ses fonctions dans les cas suivants:

- a) il ou elle est durablement incapable d'exercer ses tâches au sens de la législation sur le personnel;
- b) il ou elle a violé gravement ses devoirs de fonction de manière intentionnelle ou par négligence grave.

⁴ La décision de relever le ou la préposé-e de ses fonctions conformément à l'alinéa 3 let. b est de la compétence du Conseil d'Etat. Cette décision peut être prise à l'initiative du Conseil d'Etat ou de la Commission. Dans tous les cas, le Conseil d'Etat sollicite le préavis de la Commission.

Art. 53 Préposé-e – Empêchement

¹ En cas d'empêchement durable du ou de la préposé-e, le Conseil d'Etat désigne une personne ad interim. La procédure de désignation est menée conjointement par la Commission et la Direction à laquelle l'Autorité est rattachée.

² En cas d'empêchement ponctuel, il ou elle est remplacé-e par une personne désignée à cet effet par la Commission.

Art. 54 Préposé-e – Tâches

¹ Le ou la préposé-e a notamment pour tâches:

- a) de contrôler l'application de la législation relative à la protection des données, notamment en procédant à des vérifications auprès des organes concernés;
- b) de rendre des avis et des conseils sur les traitements de données qui lui sont présentés, du point de vue juridique et/ou technique;
- c) de prendre position et, au besoin, de proposer des mesures appropriées lorsque l'Autorité de surveillance est consultée suite à la réalisation d'une analyse d'impact relative à la protection des données;
- d) d'informer et de conseiller les organes publics dans le domaine de la protection des données et de les assister, notamment lors de l'étude de projets de traitement;
- e) de participer à la formation des organes publics aux questions de protection des données;
- f) de sensibiliser le public aux questions de protection des données et de renseigner les personnes concernées sur leurs droits;
- g) de traiter les demandes et les plaintes adressées par les personnes concernées à l'Autorité de surveillance lorsqu'elles concernent des questions de protection des données;
- h) de tenir le registre des activités de traitement prévu à l'article 38;
- i) d'apporter son concours lors de violations de la sécurité des données personnelles faisant l'objet d'une annonce conformément à l'article 43 al. 3;
- j) de veiller à ce que les échanges transfrontières de données se fassent dans un cadre qui respecte les droits des personnes concernées;
- k) de rendre des recommandations à l'attention des organes publics qui traitent des données personnelles, lorsqu'il apparaît qu'une ou plusieurs dispositions de protection des données ne sont pas respectées;
- l) de collaborer avec le Préposé fédéral à la protection des données et à la transparence ainsi qu'avec les autorités de surveillance de la protection des données des autres cantons et avec celles de l'étranger;
- m) d'exécuter tous les travaux qui lui sont confiés par la Commission;
- n) de faire rapport à la Commission sur son activité et ses constatations.

Art. 55 Autocontrôle de l'Autorité de surveillance

¹ L'Autorité de surveillance 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.

5.2 Pouvoir de contrôle et d'intervention

Art. 56 Contrôle par le ou la préposé-e

¹ Le ou la préposé-e est habilité-e à effectuer d'office ou sur plainte un contrôle auprès d'un responsable du traitement ou d'un sous-traitant afin de vérifier qu'il respecte les dispositions de protection des données.

² Il ou elle peut notamment demander des renseignements, exiger la production de documents, procéder à des inspections et se faire présenter des traitements de données.

³ Le secret de fonction et les autres obligations de confidentialité ne peuvent pas lui être opposés. Le secret professionnel demeure toutefois réservé.

⁴ Lorsque le ou la préposé-e procède à un contrôle sur la base d'une plainte de la personne concernée, il ou elle informe cette dernière des suites données à sa plainte et du résultat d'une éventuelle enquête. La personne concernée n'a pas qualité de partie à la procédure.

Art. 57 Recommandations du ou de la préposé-e

¹ En cas de violation ou de risque de violation des prescriptions sur la protection des données, le ou la préposé-e peut adresser une recommandation à l'organe public concerné l'invitant à prendre, dans un délai déterminé, les mesures nécessaires pour remédier à la situation.

² Lorsque l'organe concerné est une unité subordonnée, la recommandation est directement adressée à l'organe hiérarchiquement supérieur.

³ L'organe destinataire de la recommandation adopte, dans le délai imparti par le ou la préposé-e, une détermination sur la suite qu'il entend donner à la recommandation et la communique au ou à la préposé-e. L'absence de détermination est considérée comme un rejet de la recommandation.

⁴ En cas de rejet, total ou partiel, de la recommandation, le ou la préposé-e peut transmettre l'affaire à la Commission pour qu'elle rende une décision.

⁵ Lorsque, durant la procédure, l'organe public a pris les mesures nécessaires au rétablissement d'une situation conforme aux prescriptions de protection des données, le ou la préposé-e met un terme à la procédure et renonce à émettre une recommandation.

Art. 58 Décision de la Commission

¹ La Commission statue dans les affaires que le ou la préposé-e lui transmet conformément à l'article 57 al. 4.

² Lorsqu'un organe soumis à la présente loi ne respecte pas des dispositions de protection des données, la Commission peut ordonner la suspension, la modification ou la cessation de tout ou partie du traitement ainsi que l'effacement ou la destruction de tout ou partie des données personnelles.

³ En cas de menace grave imminente ou de violation de la protection des données susceptible de causer une atteinte grave aux droits d'une ou plusieurs personnes concernées, la Commission peut ordonner, d'office ou sur demande du ou de la préposé-e, des mesures provisionnelles urgentes pour limiter ou suspendre le traitement des données litigieux jusqu'à ce qu'elle se soit prononcée sur le fond.

⁴ Le ou la préposé-e participe avec voix consultative à la procédure devant la Commission. Il ou elle peut être chargé-e de l'instruction de l'affaire.

⁵ Lorsque, durant la procédure, l'organe public concerné a pris les mesures nécessaires au rétablissement d'une situation conforme aux prescriptions de protection des données, la Commission peut classer l'affaire ou se limiter à prononcer un avertissement

Art. 59 Procédure

¹ La procédure est régie par le code de procédure et de juridiction administrative. Sous réserve de l'article 58 al. 3, l'organe concerné bénéficie, en particulier, du droit d'être entendu.

² L'organe public visé par une décision de la Commission a qualité pour recourir contre celle-ci.

Art. 60 Coopération avec d'autres autorités de protection des données en Suisse et à l'étranger

¹ Dans l'exercice de ses fonctions, l'Autorité de surveillance peut coopérer avec les autorités cantonales, fédérales et étrangères chargées de la protection des données.

² Elle peut échanger des informations ou des données personnelles avec une autre autorité chargée de la protection des données pour l'accomplissement de leurs tâches légales respectives, 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 de collaboration;

- c) les informations et les données personnelles ne sont communiquées à des tiers qu'avec l'accord préalable de l'autorité qui les a transmises;
- d) l'autorité destinataire s'engage à ne pas communiquer plus loin les secrets professionnels, d'affaires ou de fabrication;
- 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 à caractère personnel.

³ Avant de transmettre à une autre autorité chargée de la protection des données des informations susceptibles de contenir des secrets professionnels, de fabrication ou d'affaires, l'Autorité 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.

6 Dispositions finales et transitoires

Art. 61 Règlementation d'exécution

¹ Le Conseil d'Etat adopte les dispositions nécessaires à la mise en œuvre de la présente loi. Celles-ci concernent notamment:

- a) les mesures de sécurité;
- b) l'exercice des droits des personnes concernées;
- c) la réalisation de projets pilotes;
- d) le statut et les tâches des correspondants et des correspondantes à la protection des données;
- e) les rapports de travail des membres de l'Autorité de surveillance.

Art. 62 Droit transitoire

¹ Pour les traitements déjà en cours au moment de l'entrée en vigueur de la présente loi, les responsables de traitements disposent d'un délai de deux ans pour se mettre en conformité avec les nouvelles exigences prescrites. Les articles 43 et 44 sont directement applicables.

² Pour autant que les finalités du traitement restent inchangées et que de nouvelles données ne soient pas collectées justifiant la réalisation d'une analyse d'impact, les articles 41 et 42 ne sont pas applicables aux traitements qui ont débuté avant l'entrée en vigueur de la présente loi.

³ Les traitements achevés au moment de l'entrée en vigueur de la présente loi sont régis par l'ancien droit, sauf en ce qui concerne les droits de la personne concernée (section 3).

⁴ Les articles 12, 13, 40, 41 et 42 sont applicables aux activités de traitement régis par la directive (UE) 2016/680 ²⁾ dès l'entrée en vigueur de la présente loi.

Art. 63 Adaptation de la législation

¹ Les Directions disposent d'un délai de deux ans à compter de l'entrée en vigueur de la présente loi pour adapter la législation dont elles sont en charge aux exigences de l'article 5.

Art. 64 Rapports de service du ou de la préposé-e

¹ Au moment de l'entrée en vigueur de la loi, l'autorité d'engagement adapte le contrat de travail de la personne en poste aux exigences de la nouvelle loi conformément à la législation sur le personnel.

² En cas de refus de la proposition visant à transformer le contrat de travail, la situation est réglée conformément aux dispositions en matière de suppression de poste au sens de la législation sur le personnel.

II.

1.

L'acte RSF [110.1](#) (Loi sur la statistique cantonale (LStat), du 07.02.2006) est modifié comme il suit:

Art. 5 al. 1 (*modifié*)

¹ La collecte des données respecte les principes généraux de proportionnalité et de nécessité; elle est conforme à la législation sur la protection des données.

Art. 16 al. 2 (*modifié*), **al. 3** (*modifié*)

² La publication de données personnelles ou de résultats qui permettent l'identification ou la déduction d'informations sur la situation individuelle des personnes physiques ou morales concernées est interdite conformément à l'article 26 al. 1 let. d de la loi du xx.xx.xxxx sur la protection des données.

³ Les données recueillies à des fins statistiques sont traitées confidentiellement et conformément à la législation sur la protection des données.

²⁾ Note d'auteur: 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, JO L 119 du 4.5.2016, p. 89.

2.

L'acte RSF [122.0.1](#) (Loi sur l'organisation du Conseil d'Etat et de l'administration (LOCEA), du 16.10.2001) est modifié comme il suit:

Art. 58a (nouveau)

Systemes de gestion des affaires

¹ Les Directions et les unités administratives peuvent gérer des systèmes d'information et de documentation permettant d'assurer le bon déroulement de leurs processus opérationnels ainsi que la gestion de la correspondance et d'autres documents.

² Ces systèmes peuvent contenir des données personnelles, y compris des données personnelles sensibles, dans le but de:

- a) traiter des affaires qui sont du ressort de l'organe concerné;
- b) organiser le déroulement du travail;
- c) constater si des données se rapportant à une personne déterminée sont traitées;
- d) faciliter l'accès à la documentation.

³ Le Conseil d'Etat édicte des dispositions d'exécution concernant le fonctionnement du système de gestion des affaires centralisé de l'Etat.

3.

L'acte RSF [130.1](#) (Loi sur la justice (LJ), du 31.05.2010) est modifié comme il suit:

Art. 46a (nouveau)

Correspondant ou correspondante à la protection des données

¹ Le Tribunal cantonal désigne un correspondant ou une correspondante à la protection des données au sens de l'article 45 de la loi du xx.xx.xxxx sur la protection des données (LPrD).

² Il ou elle a pour tâches de:

- a) conseiller et sensibiliser les cours et les services centraux du Tribunal cantonal en matière de protection des données;
- b) collaborer à l'élaboration des analyses d'impact au sens de la législation sur la protection des données;
- c) traiter les demandes des personnes concernées relatives au traitement de leurs données;
- d) répondre aux demandes de l'Autorité cantonale de surveillance en matière de protection des données.

³ Le correspondant ou la correspondante à la protection des données n'intervient pas dans les affaires juridictionnelles en cours.

Art. 71a (nouveau)

Correspondant ou correspondante à la protection des données

¹ Le Ministère public désigne un correspondant ou une correspondante à la protection des données au sens de l'article 45 LPrD.

² Il ou elle a pour tâches de:

- a) conseiller et sensibiliser le personnel du Ministère public en matière de protection des données;
- b) collaborer à l'élaboration des analyses d'impact au sens de la législation sur la protection des données;
- c) traiter les demandes des personnes concernées relatives au traitement de leurs données;
- d) répondre aux demandes de l'Autorité cantonale de surveillance en matière de protection des données.

³ Le correspondant ou la correspondante à la protection des données n'intervient pas dans les affaires juridictionnelles en cours.

Art. 140 al. 1

¹ Après la clôture de la procédure pénale, le traitement et la conservation des données sont régis par les dispositions fédérales et au surplus:

- a) (*modifié*) par la législation cantonale sur la protection des données;
- b) (*modifié*) par la législation cantonale sur la sécurité de l'information;
- c) (*modifié*) par la législation cantonale sur l'archivage, y compris les directives du Tribunal cantonal dans ce domaine.

4.

L'acte RSF [140.1](#) (Loi sur les communes (LCo), du 25.09.1980) est modifié comme il suit:

Art. 102a (nouveau)

Systèmes de gestion des affaires

¹ Les communes peuvent gérer des systèmes d'information et de documentation permettant d'assurer le bon déroulement de leurs processus opérationnels ainsi que la gestion de leur correspondance et d'autres documents.

² Ces systèmes peuvent contenir des données personnelles, y compris des données personnelles sensibles, dans le but:

- a) de traiter des affaires qui sont du ressort de l'organe concerné;
- b) d'organiser le déroulement du travail;
- c) de constater si des données se rapportant à une personne déterminée sont traitées;
- d) de faciliter l'accès à la documentation.

³ La législation sur la protection des données est réservée.

Art. 126 al. 1 (modifié)

¹ Les dispositions de la présente loi relatives au personnel communal (art. 69 à 76), à la représentation (art. 83), au secret de fonction (art. 83b), à la responsabilité civile (art. 83c), aux actes communaux (art. 84 à 86), aux travaux, fournitures et services (art. 99), à la tenue de systèmes de gestion des affaires (art. 102a), aux archives (art. 103) et au droit de consultation (art. 103^{bis}) sont applicables aux associations de communes.

5.

L'acte RSF [150.1](#) (Code de procédure et de juridiction administrative (CPJA), du 23.05.1991) est modifié comme il suit:

Art. 66a (nouveau)

Soutien automatisé à la prise de décision

¹ Si une autorité utilise des algorithmes pour l'aider à former son raisonnement en fait ou en droit lors de la prise d'une décision, elle est tenue d'en faire mention systématiquement dans la partie de la décision qui contient la motivation.

² A la demande du ou de la destinataire de la décision, l'autorité lui communique sous une forme intelligible la logique et les critères des algorithmes utilisés.

³ La demande n'a pas d'effet suspensif, sauf décision contraire de l'autorité, et elle n'entraîne aucune interruption de délai.

Art. AI-4a (nouveau)

Décisions individuelles automatisées

¹ Si une décision au sens de l'article 4 est prise sur le seul fondement d'un traitement de données personnelles automatisé, elle doit obligatoirement être présentée comme telle.

² A la demande de la personne faisant l'objet d'une décision automatisée, l'organe qui a émis la décision lui communique sous une forme intelligible la logique et les critères à la base de celle-ci.

³ Sauf dans les cas où il n'existe pas de droit d'être entendu avant la décision, toute personne faisant l'objet d'une décision individuelle automatisée peut, dans les 30 jours, déposer une réclamation auprès de l'organe qui l'a émise, lorsque:

- a) la décision est selon toute vraisemblance entachée d'une erreur non juridique, et
- b) l'erreur en question est imputable à la machine qui l'a rendue.

⁴ L'organe qui a émis la décision procède à un réexamen sommaire et gratuit des opérations de traitement accomplies.

6.

L'acte RSF [17.3](#) (Loi sur la vidéosurveillance (LVid), du 07.12.2010) est modifié comme il suit:

Art. 3 al. 2 (modifié)

² Les systèmes de vidéosurveillance sans enregistrement doivent, avant leur mise en service, être annoncés au préfet ou à la préfète ainsi qu'au ou à la préposé-e à la transparence et à la protection des données (ci-après: le ou la préposé-e).

Art. 4 al. 3 (nouveau)

³ Une analyse d'impact au sens de l'article 41 de la loi du xx.xx.xxxx sur la protection des données doit être réalisée avant toute installation d'un nouveau système de surveillance systématique de grandes parties du domaine public.

Art. 5 al. 1, al. 2 (modifié) [DE: (inchangé)]

¹ L'installation d'un système de vidéosurveillance avec enregistrement doit en outre faire l'objet d'une autorisation dont l'octroi est subordonné aux conditions suivantes:

- b) (inchangé) [DE: (modifié)] les mesures énoncées dans le règlement d'utilisation paraissent suffisantes pour assurer le respect des exigences générales et la protection des données.
- c) (nouveau) dans les cas visés à l'article 4 al. 3, l'analyse d'impact a été réalisée et ses conclusions sont connues.

² Le préfet ou la préfète est l'autorité compétente pour délivrer l'autorisation; il ou elle statue après avoir pris le préavis de l'Autorité cantonale de la transparence, de la protection des données et de la médiation et, le cas échéant, de la commune sur le territoire de laquelle l'installation est envisagée. Les organes de préavis reçoivent une copie de la décision.

Art. 6 al. 1 (modifié) [DE: (inchangé)]

¹ Le préfet ou la préfète exerce un contrôle général sur les systèmes de vidéo-surveillance soumis à autorisation.

Art. 7 al. 1 (modifié)

¹ Les organes publics et les personnes privées qui veulent mettre en place une vidéosurveillance d'observation sans enregistrement doivent en informer au préalable le préfet ou la préfète et le ou la préposé-e. Les organes publics informent simultanément la Direction du Conseil d'Etat dont ils dépendent ou à laquelle ils sont rattachés ou dont relève l'activité exercée dans les lieux placés sous vidéosurveillance.

7.

L'acte RSF [17.5](#) (Loi sur l'information et l'accès aux documents (LInf), du 09.09.2009) est modifié comme il suit:

Art. 33 al. 1 (modifié), **al. 2** (modifié)

¹ La personne qui a demandé l'accès et les tiers qui ont fait opposition peuvent, dans les trente jours qui suivent la détermination de l'organe public, déposer contre celle-ci une requête en médiation auprès du ou de la préposé-e à la transparence et à la protection des données (ci-après: le ou la préposé-e).

² Lorsque la médiation n'aboutit pas, le ou la préposé-e établit à l'intention des parties une recommandation écrite.

Art. 39 al. 2 (modifié)

² L'Autorité cantonale exerce les tâches qui lui incombent en vertu de la présente loi par l'intermédiaire de la Commission cantonale et du ou de la préposé-e; pour le reste et sous réserve des dispositions qui suivent, elle est régie par la législation sur la protection des données.

Art. 40 al. 1

¹ Dans le domaine du droit d'accès aux documents officiels, la Commission cantonale de la transparence, de la protection des données et de la médiation a pour tâches:

b) (modifié) de diriger l'activité du ou de la préposé-e;

b^{bis}) *Abrogé*

Art. 41 al. 1 (abrogé), **al. 2** (modifié)

Organes spécialisés – Préposé-e à la transparence et à la protection des données (*titre médian modifié*)

¹ *Abrogé*

² En vertu de la présente loi, le ou la préposé-e au sens de l'article 52 de la loi du xx.xx.xxxx sur la protection des données a en particulier pour tâches:

... (énumération inchangée)

Art. 42a (nouveau)

Droit transitoire relatif à la modification du xx.xx.xxxx – Rapports de service du ou de la préposé-e

¹ Au moment de l'entrée en vigueur de la loi, l'autorité d'engagement adapte le contrat de travail de la personne en poste aux exigences de la nouvelle loi conformément à la législation sur le personnel.

² En cas de refus de la proposition visant à transformer le contrat de travail, la situation est réglée conformément aux dispositions en matière de suppression de poste au sens de la législation sur le personnel.

8.

L'acte RSF [181.1](#) (Loi sur la médiation administrative (LMéd), du 25.06.2015) est modifié comme il suit:

Art. 5 al. 1 (modifié)

Nomination et statut (*titre médian modifié*)

¹ Le médiateur ou la médiatrice cantonal-e est nommé-e pour une période individuelle de 5 ans, reconductible. Les articles 51 à 53 de la loi du xx.xx.xxxx sur la protection des données lui sont applicables par analogie.

Art. 6 al. 2 (modifié) [DE: (inchangé)]

² Dans le domaine de la médiation, la Commission cantonale de la transparence, de la protection des données et de la médiation (ci-après: la Commission) a pour tâches:

- b) (*modifié*) de mener en collaboration avec la Direction à laquelle elle est rattachée la procédure de nomination du médiateur ou de la médiatrice cantonal-e pour le Conseil d'Etat et de préavisier à son intention la ou les candidatures privilégiées;

Art. 8

Abrogé

Art. 9

Abrogé

Art. 27 (nouveau)

Droit transitoire relatif à la modification du xx.xx.xxxx – Rapports de service du médiateur ou de la médiatrice cantonal-e

¹ Au moment de l'entrée en vigueur de la loi, l'autorité d'engagement adapte le contrat de travail de la personne en poste aux exigences de la nouvelle loi conformément à la législation sur le personnel.

² En cas de refus de la proposition visant à transformer le contrat de travail, la situation est réglée conformément aux dispositions en matière de suppression de poste au sens de la législation sur le personnel.

9.

L'acte RSF [184.1](#) (Loi sur la cyberadministration (LCyb), du 18.12.2020) est modifié comme il suit:

Art. 3 al. 1

¹ Dans la présente loi, le terme ou l'expression:

- g) (*modifié*) «externalisation» désigne une forme qualifiée de sous-traitance impliquant l'utilisation de ressources informatiques accessibles à distance, via un réseau de communication, pour stocker, traiter et partager des données;

Art. 30 al. 2 (*modifié*), **al. 3** (*modifié*)

² Au sein de l'administration cantonale, la responsabilité de la mise en œuvre et du suivi des règles de la présente section est assumée conjointement par l'autorité administrative et par le service en charge de l'informatique³). Sont réservés les cas dans lesquels l'autorité administrative gère de manière autonome tout ou partie de ses systèmes informatiques.

³ Lorsque l'externalisation concerne plusieurs autorités différentes au sein d'une même collectivité publique, une autorité principalement responsable est désignée. L'alinéa 2 s'applique pour le surplus.

Art. 35 al. 1 (*modifié*), **al. 2** (*nouveau*), **al. 3** (*nouveau*)

Projets pilotes – Principes (*titre médian modifié*)

¹ Dans le but d'expérimenter l'intégration de nouveaux processus électroniques et/ou de nouvelles technologies dans le fonctionnement et l'organisation de l'administration, le Conseil d'Etat est autorisé par le biais d'une ordonnance pilote à déroger temporairement et de manière limitée à une règle de droit qui entrerait en conflit avec la poursuite de l'expérimentation.

³) Actuellement: Service de l'informatique et des télécommunications.

² La réalisation d'un projet pilote est soumise aux conditions suivantes:

- a) le projet sert à l'accomplissement d'une tâche décrite dans une loi au sens formel, poursuit un intérêt public avéré et/ou fait partie d'un projet stratégique mené conjointement entre les organes de la Confédération, des cantons et/ou des communes;
- b) des mesures appropriées sont prises aux fins de prévenir les risques d'atteinte aux droits fondamentaux des personnes concernées;
- c) une phase d'essai s'avère indispensable avant l'entrée en vigueur de la loi au sens formel, en particulier pour des raisons organisationnelles et/ou techniques;
- d) le projet pilote fait l'objet d'un dossier complet qui décrit son but, son périmètre, le besoin d'évaluation, les normes auxquelles il déroge, les mesures prises pour prévenir les éventuels risques d'atteinte aux droits fondamentaux des personnes concernées, l'organe responsable, la planification et les conséquences financières envisagées.

³ Le traitement automatisé de données personnelles dans des projets pilotes est en outre régi par la loi sur la protection des données, en particulier son article 22.

Art. 35a (nouveau)

Projets pilotes – Phase d'essai

¹ Une phase d'essai peut être considérée comme indispensable lorsque:

- a) l'accomplissement d'une tâche nécessite des innovations techniques dont les effets doivent d'abord être évalués, ou
- b) l'accomplissement d'une tâche requiert des mesures organisationnelles ou techniques importantes dont l'efficacité doit d'abord être évaluée, notamment dans le cadre de la collaboration entre organes publics.

² L'organe responsable transmet, au plus tard deux ans après la mise en œuvre de la phase d'essai, un rapport d'évaluation au Conseil d'Etat. Dans ce rapport, il lui propose la poursuite ou l'interruption de l'expérimentation.

³ Si le Conseil d'Etat autorise la poursuite de l'expérimentation, il engage immédiatement la procédure législative visant à adopter les bases légales formelles nécessaires. Il transmet au Grand Conseil un projet de loi, en principe, dans un délai de cinq ans suivant le début du projet pilote.

Art. 35b (nouveau)

Projets pilotes – Dispositions diverses

¹ Dans la mesure où elle est exigée, l'article 35 vaut base légale au sens de l'article 54 de la Constitution cantonale sur l'accomplissement de tâches par des tiers pour toute la durée du projet.

² Des essais pilotes peuvent également être menés par les communes aux mêmes conditions. La réalisation d'un essai pilote doit être prévue dans un règlement de portée générale.

10.

L'acte RSF [411.0.1](#) (Loi sur la scolarité obligatoire (loi scolaire, LS), du 09.09.2014) est modifié comme il suit:

Art. 43 al. 3a (nouveau), **al. 4** (modifié)

^{3a} Le NAVS13 peut également être transmis à des fins d'identification à la Fédération des services d'identité de l'espace suisse de formation mandatée par la Conférence suisse des directeurs cantonaux de l'instruction publique (CDIP). Le Conseil d'Etat édicte les dispositions d'exécution nécessaires.

⁴ Les données personnelles peuvent être rendues accessibles au moyen d'une procédure d'appel électronique au sens de l'article 14 al. 4 de la loi du xx.xx.xxxx sur la protection des données. Le Conseil d'Etat en fixe les modalités d'application.

11.

L'acte RSF [412.0.1](#) (Loi sur l'enseignement secondaire supérieur (LESS), du 11.12.2018) est modifié comme il suit:

Art. 43 al. 3a (nouveau), **al. 4** (modifié)

^{3a} Le numéro AVS (NAVS 13) peut également être transmis à des fins d'identification à la Fédération des services d'identité de l'espace suisse de formation mandatée par la Conférence suisse des directeurs cantonaux de l'instruction publique (CDIP). Le Conseil d'Etat édicte les dispositions d'exécution nécessaires.

⁴ Les données personnelles peuvent être rendues accessibles au moyen d'une procédure d'appel électronique au sens de l'article 14 al. 4 de la loi du xx.xx.xxxx sur la protection des données. Le Conseil d'Etat en fixe les modalités d'application.

12.

L'acte RSF [610.1](#) (Loi sur les finances de l'Etat (LFE), du 25.11.1994) est modifié comme il suit:

Intitulé de section après Art. 47 (nouveau)

6a Système de gestion intégré des finances

Art. 47a (nouveau)

But et contenu du système de gestion intégré des finances

¹ L'Administration des finances exploite un système de gestion intégré des finances pour l'accomplissement des tâches et attributions découlant de la présente loi (ci-après: le système de gestion intégré), notamment en lien avec:

- a) la gestion financière et opérationnelle;
- b) la planification financière et le suivi budgétaire.

² Le système de gestion intégré contient les données financières ainsi que les données personnelles nécessaires à l'accomplissement des tâches et attributions visées par le précédent alinéa. Les catégories de données personnelles suivantes peuvent notamment être traitées:

- a) identités et adresses des personnes physiques et des personnes morales qui ont des relations financières avec l'Etat;
- b) informations sur les coordonnées financières des personnes visées par la lettre a et sur leurs transactions financières avec l'Etat.

³ Le système de gestion intégré peut contenir des données personnelles sensibles, pour autant que l'accomplissement des tâches mentionnées à l'alinéa 1 en dépende.

Art. 47b (nouveau)

Accès au système de gestion intégré des finances

¹ Le système de gestion intégré est mis à la disposition des établissements et services pour leur permettre d'effectuer les opérations financières et comptables relevant de leurs domaines de compétence. Les communes y ont également accès pour consulter leur propre compte courant.

² Les établissements et services utilisateurs du système de gestion intégré peuvent y saisir les données, y compris des données personnelles sensibles, qu'ils traitent en lien avec la gestion et la planification financières.

³ L'Administration des finances dispose d'un accès direct et permanent à la totalité des données introduites dans le système de gestion intégré par les établissements et services utilisateurs.

⁴ Si l'accomplissement des tâches et attributions découlant de la présente loi le requiert, le système de gestion intégré peut être interfacé avec d'autres systèmes d'information de l'Etat. Une autorisation préalable est requise et les droits d'accès doivent être strictement délimités.

⁵ Les données personnelles peuvent être rendues accessibles au moyen d'une procédure d'appel au sens de la loi cantonale sur la protection des données.

⁶ Les données personnelles contenues dans le système de gestion intégré peuvent, sur demande, être communiquées à d'autres autorités ou à des tiers lorsque cette communication est nécessaire à l'accomplissement des tâches et attributions découlant de la présente loi.

Art. 47c (nouveau)

Mesures de sécurité et responsabilité

¹ Le Conseil d'Etat précise les mesures de sécurité de l'information à appliquer ainsi que la répartition des responsabilités entre les diverses entités concernées.

² Le détail des mesures de sécurité à mettre en œuvre ainsi que celui de la répartition des responsabilités peut être fixé dans des conventions passées entre l'Administration des finances et les établissements et services utilisateurs du système de gestion intégré. Les conventions sont transmises pour information à l'Autorité cantonale de la transparence, de la protection des données et de la médiation.

13.

L'acte RSF [821.0.1](#) (Loi sur la santé (LSan), du 16.11.1999) est modifié comme il suit:

Art. 60 al. 3 (modifié)

³ Si le ou la professionnel-le de la santé a des raisons de craindre que la consultation du dossier ne puisse avoir de graves conséquences pour le patient ou la patiente, il ou elle peut proposer que la consultation n'ait lieu qu'en sa présence ou celle d'un ou d'une autre professionnel-le désigné-e par le patient ou la patiente.

III.

L'acte RSF [17.1](#) (Loi sur la protection des données (LPrD), du 25.11.1994) est abrogé.

IV.

La présente loi est soumise au referendum législatif. Elle n'est pas soumise au referendum financier.

Le Conseil d'Etat fixe la date d'entrée en vigueur de la présente loi.