CANTON DU VALAIS
KANTON WALLIS

Présidence du Conseil d'Etat
Chancellerie d'Etat
Service administratif et juridique

Präsidium des Staatsrates
Staatskanzlei
Verwaltungs- und Rechtsdienst

Rapport explicatif

accompagnant l'avant-projet sur la révision de la loi sur l'information du public, la protection des données et l'archivage

Introduction

Le député Sébastien Nendaz a déposé le 9 mai 2019 une motion demandant au Conseil d'Etat de revoir les différentes interprétations de la loi sur l'information du public, la protection des données et l'archivage du 9 octobre 2008 (LIPDA / RS 170.2), afin de clarifier les compétences et l'organisation de la Commission cantonale de la protection des données et de la transparence et de se mettre en conformité avec le droit fédéral et avec la loi sur la protection des données Schengen. Le Conseil d'Etat a décidé le 5 février 2020 d'entamer les travaux de révision de la LIPDA et ce dans le but de s'aligner sur le droit fédéral mais aussi sur les textes européens.

La LIPDA est restée en effet quasiment inchangée depuis son adoption.

Les lois en matière de protection des données ont pourtant fortement évolué. Le Conseil fédéral a soumis le 15 septembre 2017 au Parlement fédéral un projet de révision totale de la Loi fédérale sur la protection des données (LPD) et sur la modification d'autres lois fédérales. Les travaux relatifs à la révision LPD (nLPD) sont terminés. Au niveau européen, c'est l'adoption le 27 avril 2016 du Règlement général sur la protection des données (RGPD)[1] qui a reçu le plus d'attention. Il s'applique désormais directement dans tout l'Espace économique européen et déploie aussi des effets en Suisse dans certaines situations spécifiques[2].

Le Protocole portant amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[3] conclu à Strasbourg le 10 octobre 2018 a été signé par la Confédération. L'Arrêté fédéral relatif

[1] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.
[2] Application extraterritoriale au sens de l'art. 3 al. 2 RGPD.
[3] Convention 108+ ou Convention 108 modernisée.

à l'approbation a été adopté par le Conseil National le 11 mars 2020 et le Conseil des Etats le 2 juin 2020. Ce protocole d'amendement modernise la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981[4] afin de répondre aux défis que soulèvent l'utilisation des nouvelles technologies et les flux toujours plus importants de données pour la protection de la sphère privée.

Ces dispositions ne sont cependant pas directement applicables et doivent donc être transposées en droit national et cantonal. L'adaptation au niveau fédéral se fait dans le cadre de la révision totale de la LPD. Les cantons doivent faire de même pour leurs législations respectives.

Finalement, la Directive (UE) 2016/680 adoptée le 27 avril 2016 et 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 a reçu moins d'attention du grand public. Elle n'en joue pas moins un rôle important pour l'administration et a conduit au niveau fédéral à l'adoption de la Loi sur la protection des données Schengen (LPDS) le 28 septembre 2018. Les cantons sont également occupés de mettre à jour leurs lois dans ce cadre.

La présente révision ne porte pas sur le volet relatif à l'information du public de la LIPDA, mais prévoit une mise à jour générale des dispositions en matière de protection des données pour tenir compte de la Convention 108, de la révision totale de la LPD, du RGPD et de la Directive (UE) 2016/680.

Comme il ne s'agit pas d'une révision totale, la structure de la loi a été conservée.

L'accès aux documents officiels n'est en principe pas modifié, sauf quelques adaptations apportées en particulier lorsque des dispositions communes régissaient l'accès aux données à caractère personnel et aux documents officiels et la procédure.

1. Commentaire des dispositions

1.1 Article 1

Les notions d'organe(s) et d'organe(s) public(s) ont été remplacées dans l'ensemble de la loi, ainsi que dans le règlement d'exécution, par celle d'autorité(s) afin

[4] Convention 108.

d'uniformiser la terminologie. Le terme d'autorité(s) est gardé conformément à l'ancienne loi.

Le but de la LIPDA reste inchangé en ce qui concerne la protection des données. La LIPDA concrétise sur le plan légal le droit à l'autodétermination en matière informationnelle, à savoir le droit pour la personne concernée de pouvoir déterminer elle-même si et dans quels buts des informations à son sujet peuvent être traitées, quelle que soit sa nationalité ou son lieu de résidence.

1.2 Article 2

Afin de tenir compte des modifications apportées à la loi, les renvois prévus à l'art. 2 al. 2 ont été modifiés. En ce qui concerne l'art. 2 al. 3, la notion de traitement vient remplacer celle de fichier. Pour ne pas limiter l'exception de l'art. 2 al. 3 aux seuls traitements relevant de la santé publique, de la police judiciaire ou des tribunaux, ces mentions ont été supprimées. L'adoption d'une loi spéciale régissant le traitement de données à caractère personnel dans un domaine spécifique reste ainsi possible, mais elle doit évidemment être conforme aux exigences constitutionnelles et respecter les exigences de la Convention 108+ et de la CEDH.

1.3 Article 3

Les définitions sont adaptées à l'évolution technologique et à la terminologie utilisée par la nLPD et le RGPD.

Al. 3 Donnée à caractère personnel (donnée)

Il n'y a pas de différence entre la notion de donnée(s) personnelle(s) figurant dans la LPD et celle de donnée(s) à caractère personnel figurant dans la LIPDA, le RGPD et d'autres lois cantonales. Dans un but de clarification, la notion de donnée(s) personnelle(s) parfois utilisée a été remplacée dans l'ensemble de la loi et du règlement d'exécution par celle de donnée(s) à caractère personnel ou simplement par celle de donnée(s).

Cet alinéa mentionne non seulement la notion de donnée, mais également celle de personne concernée. Afin d'uniformiser la terminologie, la notion de personne concernée est utilisée uniquement au singulier dans l'ensemble de la loi et de son règlement d'exécution.

Le projet renonce à la protection des données des personnes morales et s'aligne ainsi sur la nLPD et sur les textes de protection des données de l'UE, du Conseil de l'Europe et de la majorité des pays étrangers. La protection de la personnalité et des droits fondamentaux des personnes morales demeure au travers d'autres normes (protection de la personnalité, concurrence déloyale, droit d'auteur). Ce renoncement facilitera grandement le transfert de données à l'étranger et limitera les obligations à

charge des autorités pour des données qui sont souvent en partie déjà publiquement accessibles.

En ce qui concerne le secteur public, l'abrogation de la protection des données des personnes morales a pour conséquence que les bases légales prévues par le droit cantonal qui habilitent les autorités à traiter des données à caractère personnel ne concernent désormais plus que les données de personnes physiques. Or l'activité de l'Etat doit être régie par la loi. Les différentes normes de droit cantonal qui autorisent un traitement de données à caractère personnel devront donc être adaptées pour justifier l'atteinte à la personnalité et aux droits fondamentaux des personnes morales. Afin d'éviter des lacunes juridiques, une disposition transitoire est adoptée pour une durée de cinq ans (art. T1-1).

L'art. 25 al. 8 RELIPDA concernant la consultation des données d'une personne décédée doit être supprimée. Elle ne repose sur aucune disposition de la LIPDA. Selon le code civil (CC), la personnalité finit par la mort (art. 31 al. 1 CC). Dans le cadre de la révision de la LPD, le parlement fédéral a refusé les dispositions sur les données de personnes décédées. Une disposition similaire à celle de l'art. 25 al. 8 du RELIPDA est certes utile, mais devrait figurer dans le code civil ou une autre loi.

Al. 4 Traitement

La définition du « traitement » n'est pas modifiée, mais les exemples non exhaustifs de traitements sont mis à jour pour correspondre à la réalité technique et se rapprocher de la nLPD et des textes européens. La définition du « traitement » continue à englober toutes les opérations effectuées sur les données, qu'elles le soient de façon totalement automatisée ou en partie seulement. Vu que la notion de fichier est abandonnée, il est expressément prévu que, lorsqu'aucun procédé automatisé n'est utilisé, le traitement de données désigne une opération sur des données à caractère personnel au sein d'un ensemble structuré de données qui sont accessibles ou peuvent être retrouvées selon des critères spécifiques et qui permettent au responsable du traitement ou à toute autre personne de rechercher, combiner ou mettre en corrélation des données relatives à une personne. Cette précision ressort de l'art. 2 let. c de la Convention 108+.

Al. 6 Responsable du traitement

La notion de fichier qui figurait à l'al. 5 est supprimée, car elle ne joue plus grand rôle et n'est pas nécessaire.

La notion de « maître du fichier », qui figurait à l'ancien al. 6 est remplacée par celle plus universelle de « responsable du traitement » connue de la nLPD, du RGPD et de plusieurs lois cantonales, sans modification matérielle de sa portée. Les modifications se retrouvent dans l'ensemble de la loi et de son règlement d'exécution.

Al. 6bis Sous-traitant

La sous-traitance étant traitée à l'art. 29, il est nécessaire d'ajouter la définition du sous-traitant à l'art. 3. Le sous-traitant est celui qui traite des données pour le compte du responsable du traitement. Le sous-traitant peut être une personne privée (personne physique ou morale) ou une autorité.

Al. 6ter Destinataire

La notion de destinataires est prévue dans plusieurs dispositions de la loi. Afin d'interpréter cette notion de manière constante, sa définition est également introduite à l'art. 3, le destinataire étant celui qui reçoit communication des données. Le destinataire peut être une personne privée (personne physique ou morale) ou une autorité, agissant comme responsable du traitement, sous-traitant ou tiers.

Al. 7 Données sensibles

Conformément à la nLPD et au droit européen, la notion de « données sensibles » est étendue aux « données concernant les opinions et activités philosophiques », aux « données concernant la vie sexuelle », aux « données concernant l'origine ethnique », aux « données génétiques » et aux « données biométriques identifiant un individu de façon unique ». La notion suisse de données sensibles a été préférée à celle de catégories particulières de données à caractère personnel du RGPD.

Les données génétiques sont les informations relatives au patrimoine génétique d'une personne obtenues par une analyse génétique, y compris le profil d'ADN[5].

Par données biométriques, on entend ici les données à caractère personnel résultant d'un traitement technique spécifique et relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment son identification unique, comme des empreintes digitales, des images faciales, l'iris, ou encore la voix. Ces données doivent impérativement résulter d'un traitement technique spécifique qui permet l'identification ou l'authentification unique d'un individu. Tel ne sera en principe pas le cas, par exemple, de simples photographies.

Al. 8 Profilage

La notion statique et dépassée de « profil de la personnalité » qui constitue une particularité suisse disparaît également au profit de la notion dynamique de « profilage », comme dans la nLPD.

Le profilage est une forme particulière de traitement orienté vers une finalité particulière. Il peut être défini comme l'évaluation de certaines caractéristiques d'une personne sur la base de données à caractère personnel traitées de manière

[5] Art. 3 let. l, de la loi fédérale du 8 octobre 2014 sur l'analyse génétique humaine (LAGH).

automatisée, afin notamment 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. Autrement dit, le profilage se caractérise par le fait qu'on procède à une évaluation automatisée de données à caractère personnel afin de pouvoir évaluer, d'une manière également automatisée, les caractéristiques de la personne. On est ainsi en présence d'un profilage uniquement lorsque le processus d'évaluation est entièrement automatisé.

Al. 8bis Violation de la sécurité des données

L'introduction de l'art. 30a prévoyant l'obligation d'annoncer les violations de la sécurité des données implique de la définir préalablement. Est donc considérée comme telle toute violation de la sécurité, sans égard au fait qu'elle soit intentionnelle ou illicite, entraînant la perte de données à caractère personnel, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données.

Ce terme est évidemment lié à l'art. 21 qui prévoit que le responsable du traitement, ainsi que, le cas échéant, le sous-traitant, sont tenus de mettre en place des mesures techniques et organisationnelles respectant les prescriptions de protection des données à tous les stades du traitement.

Ce qui compte, c'est que l'événement en question ait eu lieu. Peu importe que la divulgation ou l'accès non autorisés se soient effectivement produits ou aient simplement été rendus possibles. En effet, lorsqu'un support de données a été perdu, il est souvent difficile de prouver que les données qu'il contenait ont été vues ou utilisées par des personnes non autorisées. C'est pourquoi la perte de cet objet constitue en elle-même une violation de la sécurité des données. Ce sont plutôt l'ampleur et la signification d'une telle violation qui sont déterminantes pour les mesures à prendre, en particulier pour l'estimation du risque conformément à l'art. 30a.

1.4 Article 12 alinéa 2

L'art. 12 al. 2 est modifié pour corriger une erreur concernant seulement la version française.

La notion de procédures juridictionnelles administratives pendantes figurant dans la version française ne correspond pas à la version allemande qui vise l'ensemble des procédures administratives pendantes. Une procédure juridictionnelle administrative est une procédure contentieuse dans laquelle une décision administrative de

première instance a été contestée[6]. Le Message initial, dans sa version française, faisait déjà référence à des procédures pendantes, sans distinguer selon que ces procédures sont juridictionnelles ou non, ce qui concorde avec la version allemande où cette distinction n'apparaît pas non plus.[7]

Afin d'uniformiser les versions du texte de loi, la précision « juridictionnelles » est donc supprimée de la disposition française seulement.

1.5 Article 12a

Jusqu'à présent, l'accès aux données à caractère personnel et aux documents officiels était régi par les art. 48ss, bien qu'il s'agît de buts et modalités différentes. La procédure est désormais régie dans des dispositions séparées.

Un nouvel art. 12a est intégré afin de clarifier le déroulement des demandes d'accès aux documents officiels. Il reprend le contenu des art. 48 et 49 dans la mesure où ils concernaient l'accès aux documents officiels. L'accès aux données à caractère personnel est traité dans le chapitre correspondant.

Les al. 1 à 3 correspondent pour l'essentiel à l'ancien art. 48 al. 1 à 3. Les al. 4 à 6 reprennent pour l'essentiel l'ancien art. 49 al. 1 à 3.

1.6 Article 12b

L'art. 12b correspond pour l'essentiel à l'ancien art. 50. Contrairement au délai de dix jours prévu par l'actuelle loi, l'avant-projet prévoit de porter le délai à vingt jours comme cela est prévu dans la Loi fédérale sur le principe de la transparence dans l'administration

Exceptionnellement, le délai de vingt jours peut être prolongé lorsque la demande porte sur des documents qui sont complexes, nombreux, difficiles à obtenir ou qui nécessitent un examen approfondi pour la pesée des intérêts en présence. Dès qu'elle perçoit que la demande nécessitera une prolongation du délai, l'autorité informe rapidement le demandeur de cette prolongation, de sa durée et des causes qui en sont à l'origine. L'autorité reste tenue de traiter la demande conformément au principe de célérité.

1.7 Article 13

Afin d'être plus précise, la référence à d'autres dispositions de la loi mentionnée à l'al. 2 a été modifiée pour ne contenir que l'art. 22. L'avant-projet prévoit également la possibilité de tenir compte du consentement de la personne concernée. Si le consentement n'est soumis à aucune exigence de forme, celui-ci doit toutefois respecter les critères fixés à l'art. 18 al. 4 pour être valide. Il appartient dans tous les

[6] Sébastien Fanti, *La notion de document officiel en droit fédéral, ainsi qu'en droit valaisan*, RVJ 2016 p. 410 ; Basler Kommentar zum Öffentlichkeitsgesetz, STAMM-PFISTER, 3e éd., Bâle 2014, n. 21 ad art. 3.

[7] Considérant 3.2.1 de l'arrêt précité.

cas à l'autorité de prouver l'existence du consentement, si bien qu'elle a tout intérêt à le documenter.

1.8 Article 15 alinéa 7

L'art. 15 est complété par un al. 7. Le texte de cet alinéa est repris pour l'essentiel de l'ancien art. 15. Même si l l'al. 4 ne mentionne que le refus, l'autorité peut aussi, en vertu du principe qui peut le plus peut le moins, limiter ou différer l'accès.

1.9 Article 17

Les al. 1 et 3 concernaient l'exigence de la base légale, alors que l'al. 2 traitait des principes. Pour plus de lisibilité, l'art. 17 est désormais consacré seulement à la question de la base légale.

L'al. 1 prévoit que tout traitement de données n'est autorisé que pour autant qu'il repose sur une base légale. Afin de s'aligner sur la nLPD, la mention de l'accomplissement d'une tâche légale a été biffée.

L'art. 17 est complété par de nouveaux al. 2 et 3 qui précisent quand une base légale formelle est nécessaire. L'art. 18 traite des principes et reprend en partie l'ancien art. 17 al. 2.

Une loi au sens formel est exigée, comme dans l'ancienne loi, lorsqu'il s'agit d'un traitement de données sensibles (al. 2 let. a). Cette hypothèse est également complétée par le cas du profilage (la notion de profil de personnalité qui était assimilée aux données sensibles ayant été supprimée). Il est ajouté (al. 2 let. b) qu'un traitement doit reposer sur une base légale au sens formel lorsque la finalité ou le mode du traitement de données est susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée.

L'al. 3 prévoit que des données peuvent être traitées seulement sur la base d'une loi au sens matériel lorsque le traitement ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée et que l'une des conditions alternatives des let. a à c se réalise. Il faut non seulement que le traitement en lui-même, mais également son résultat, ne présentent pas de risques particuliers. Les exceptions doivent être admises de manière limitée. Elles doivent notamment permettre d'éviter que l'autorité ne se retrouve empêchée de traiter des données uniquement parce que la loi ne le prévoit pas expressément, alors que cela correspond à l'accomplissement d'une tâche de l'autorité. La défense des intérêts vitaux vise des cas où le législateur n'a évidemment pas le temps d'adopter les bases légales et se justifie par l'importance du bien juridique à défendre. Quant au traitement de données rendues publiques par la personne concernée, il serait choquant de limiter trop fortement le traitement alors qu'elle ne s'y est pas opposée.

1.10 Article 18

L'ancien art. 18 relatif à la collecte de données est supprimé, l'obligation d'information de l'art. 19 étant renforcée et suffisante.

Les principes généraux en matière de protection des données qui figuraient partiellement à l'al. 2 de l'ancien art. 17 sont désormais énumérés à l'art. 18 al. 1 qui a aussi été complété. Ces principes doivent être respectés lors de tout traitement de données. Il s'agit de manière classique des principes de loyauté (bonne foi), transparence, finalité, proportionnalité et exactitude. La terminologie est reprise de l'art. 5 de la Convention 108+.

Principe le plus susceptible d'être violé en pratique, le principe de proportionnalité nécessite une attention particulière. Il est important de souligner que chaque traitement de données doit être proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu. Ainsi, tant le choix des moyens de traitement que les modalités du traitement ou encore son étendue doivent respecter le principe de proportionnalité.

L'art. 18 est encore complété par les obligations de protéger les données dès la conception (*privacy by design,* al. 2) et par défaut (*privacy by default,* al. 3) connues de la nLPD et du droit européen. Il ne s'agit pas à proprement parler de principes mais d'obligations qui y sont étroitement liées, raison pour laquelle il se justifie de les ajouter ici. Le responsable du traitement doit concevoir dès l'origine le traitement de données de telle manière qu'il respecte les prescriptions relatives à la protection des données. Le responsable du traitement doit mettre en œuvre, dès la conception, des moyens de traitement et lors du traitement proprement dit, des mesures techniques et organisationnelles appropriées destinées à mettre en œuvre les principes relatifs à la protection des données, telles que la pseudonymisation, ou la minimisation des données, et à assortir le traitement des garanties nécessaires. Ces mesures doivent tenir compte de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement. Ces mesures doivent être adaptées en fonction des risques que présente le traitement pour les droits et libertés des personnes.

Cette obligation repose sur le principe de la technologie au service de la protection des données. Les exigences légales auxquelles doit satisfaire un traitement conforme à la protection des données doivent être intégrées dans le système, de manière à rendre impossible une violation de la protection des données ou d'en réduire la probabilité. Il faut fixer avant même le début du traitement ses modalités, de manière

à traiter le moins de données possible, et à les conserver le moins longtemps possible (principe de la minimisation des données).

De plus, le responsable du traitement est tenu, par le biais de préréglages appropriés, de garantir que le traitement soit limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement.

Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaire au regard de chaque finalité spécifique du traitement sont traitées. Cette obligation s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. Les mesures résident dans des réglages prédéfinis qui s'appliquent de manière standardisée, lorsque l'utilisateur ne choisit pas une autre voie. Dans le contexte de la protection des données, cela signifie que le processus de traitement doit être préprogrammé de manière à garantir autant que possible la protection des données, mais qu'on laisse à la personne concernée la possibilité d'en modifier les paramètres. Le lien entre la protection des données dès la conception et par défaut est étroit, le tout étant inscrit dans un système entier respectueux de la protection des données.

La notion de consentement est précisée à l'al. 4 afin de correspondre aux exigences la Convention 108+. Le consentement de la personne concernée doit être libre, spécifique, éclairé et non équivoque. Le consentement doit représenter la libre expression d'un choix intentionnel. Cela peut se faire au moyen d'une déclaration écrite ou orale ou par une action affirmative qui indique clairement l'acceptation du traitement des données à caractère personnel. Le consentement doit couvrir l'ensemble des activités de traitement de données qui poursuivent la ou les mêmes finalités. Lorsque les finalités sont multiples, un consentement doit être donné pour chacune d'entre elles. La personne concernée doit être informée des implications de sa décision. Aucune influence ou pression indues, directe ou indirecte, ne peut être exercée sur la personne concernée.

1.11 Article 19

L'al. 2 est complété notamment conformément à l'art. 8 de la Convention 108+. Les nouvelles informations qui doivent être données à la personne concernée sont l'indication de la base légale (let. b), les données ou au moins les catégories de données traitées (let. d) et l'ensemble des droits de la personne concernée (let. e). L'obligation d'informer sur le droit d'accès n'est plus nécessaire puisqu'elle est désormais couverte par les droits de la personne concernée (droit d'accès, droit de rectification ou de destruction, etc.). Afin de tenir compte du catalogue minimum des

informations à transmettre pour garantir une transparence suffisante prévu par la Convention 108+, le responsable du traitement doit également communiquer toute autre information complémentaire nécessaire pour garantir un traitement loyal et transparent des données (let. h) à l'instar parfois de la durée de conservation du traitement.

En outre, les al. 2bis et 3 sont remodelés à des fins de clarification et de simplification.

1.12 Article 19a

Le titre de la disposition est modifié uniquement pour des questions de cohérence terminologique concernant le devoir d'informer.

L'art. 19a définit plusieurs situations dans lesquelles le responsable du traitement est complètement délié de son devoir d'informer la personne concernée. Les restrictions de l'art. 19a correspondent à ce qui est prévu par la nLPD. La transparence des traitements de données étant un principe central du droit de la protection des données, les restrictions au devoir d'informer doivent être interprétées de manière stricte.

1.13 Article 20

L'art. 20 est adapté afin de correspondre aux exigences de la Convention 108+ et aux art. 19 nLPD et 22 RGPD.

Une décision automatisée implique que la décision ne soit pas prise par une personne physique sur la base de sa propre évaluation de la situation. Il y a décision individuelle automatisée lorsqu'une exploitation de données a lieu sans intervention humaine et qu'il en résulte une décision, ou un jugement, à l'égard de la personne concernée. Le fait que la décision soit au final communiquée par une personne physique ne change rien à son caractère automatisé, car cette personne n'a pas d'influence sur le processus de décision. La question déterminante est ainsi celle de savoir dans quelle mesure une personne physique peut faire un examen de la situation et se baser sur ses propres considérations pour rendre une décision finale.

L'al. 1 exige une information de la personne concernée lorsqu'une décision est prise exclusivement sur la base d'un traitement de données à caractère personnel automatisé, et que cette décision a des effets juridiques sur la personne concernée ou qu'elle l'affecte de manière significative. Il n'est donc pas nécessaire que la personne concernée soit informée de chaque décision individuelle automatisée, mais seulement lorsque la décision a pour elle des effets juridiques ou l'affecte de manière significative. Il y a par exemple des effets juridiques lorsqu'une décision découle d'une taxation fiscale automatique. On peut supposer que la personne concernée est affectée de manière significative lorsqu'elle est durablement entravée sur le plan économique ou personnel. Une simple nuisance ne suffit pas. Tout dépend des

circonstances concrètes du cas particulier. Il faut en particulier tenir compte de l'importance de l'entrave en question pour la personne concernée, de la durée des effets de la décision et de l'existence ou non d'une solution de remplacement.

Selon l'al. 2, le responsable du traitement doit donner à la personne concernée, si elle le demande, la possibilité de faire valoir son point de vue sur le résultat de la décision, et même exiger que la décision soit revue par une personne physique. Le but est entre autres d'éviter que le traitement de données soit effectué sur la base de données incomplètes, dépassées ou non pertinentes. Cette règle est également dans l'intérêt du responsable du traitement, pour lequel une décision individuelle automatisée erronée peut avoir des conséquences négatives.

L'al. 3 précise que l'al. 2 ne s'applique pas lorsque la personne concernée dispose d'un droit de recours contre la décision, car elle peut y faire valoir son point de vue et faire examiner la décision par une personne physique. Ses droits sont donc déjà garantis.

Pour des raisons pratiques, on peut renoncer à l'obligation d'indiquer spontanément la logique sur laquelle se base la décision. Celle-ci doit en revanche être communiquée sur demande de la personne concernée et en réponse à un droit d'accès (art. 31 al. 1 let. h).

1.14 Article 21

L'art. 21 est entièrement reformulé pour tenir compte des évolutions techniques.

Les responsables du traitement et les sous-traitants doivent assurer une sécurité adéquate des données à caractère personnel par rapport au risque encouru. Cette disposition matérialise l'approche fondée sur les risques (al. 2). Plus le risque d'une atteinte à la sécurité des données est élevé, plus les exigences auxquelles doivent répondre les mesures à prendre sont élevées. Il ne s'agit pas d'un processus statique. Le risque comme les mesures prises doivent régulièrement être réévalués.

La sécurité des données doit assurer la confidentialité, la disponibilité et l'intégrité des données, ce qui inclut également la résilience des systèmes et des services de traitement.

L'al. 1 est complété par la mention de quelques mesures classiques comme la pseudonymisation et le chiffrement des données. Les mesures doivent être des mesures organisationnelles et techniques. Elles peuvent viser par exemple à sensibiliser les utilisateurs aux risques liés aux libertés et à la sphère privée, à authentifier les utilisateurs avant tout accès aux données et moyens de traitement et limiter leurs accès aux seules données nécessaires, à prévoir un système de journalisation pour tracer les accès et gérer les incidents ou certaines opérations de traitement dans des systèmes de traitement automatisé, à effecteur des sauvegardes

régulières et assurer la continuité d'activité, à archiver et détruire les données de manière sécurisée, à assurer l'intégrité et l'authenticité des données, ou encore à tester, à analyser et à évaluer régulièrement l'efficacité des mesures prises.

Il est renoncé à fixer des exigences techniques dans la loi en raison de l'évolution rapide du cadre technique. L'al. 3 donne la compétence au Conseil d'Etat pour édicter des dispositions plus précises sur les exigences minimales à respecter en matière de sécurité des données à caractère personnel. Le préposé et les services informatiques peuvent également recommander de bonnes pratiques dans leurs domaines de compétence.

Les mesures doivent être appropriées au regard notamment de l'état de la technique, du type de traitement, de son étendue ainsi que du risque que le traitement des données en question présente pour les droits fondamentaux de la personne concernée et elles doivent permettre d'éviter toute violation de la sécurité des données, soit toute violation de la sécurité entraînant la perte de données, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données, et ce indépendamment de la question de savoir si la violation est intentionnelle ou non, licite ou illicite, et si les données sont transmises, conservées ou traitées d'une autre manière.

1.15 Article 22

Les principes en matière de communication des données à caractère personnel par une autorité sont traités dans cet article. Pour être valide, le consentement doit respecter les critères fixés à l'art. 18 al. 4..

L'art. 22 est complété par un nouvel al. 1bis qui prévoit que le nom, le prénom, l'adresse et la date de naissance peuvent être communiqués sur demande et si le requérant fait valoir un intérêt légitime. Cette possibilité de communication est ajoutée en conformité avec l'art. 32 al. 4 nLPD, qui reprend une possibilité qui existait déjà depuis longtemps dans la LPD. Cette disposition a pour but de faciliter la tâche de l'autorité pour répondre à des demandes individuelles. Elle doit toutefois procéder dans chaque cas à une pesée d'intérêts, mais les exigences ne devraient pas être trop élevées vu l'atteinte en principe limitée.

La portée matérielle des l'al. 2 et 3 demeurent inchangées. Il s'agit simplement de simplifications rédactionnelles.

Le droit de s'opposer à la communication a été ajouté aux al. 4 et 5. Ce mécanisme accorde à la personne concernée le droit limité de s'opposer à une communication de données pourtant normalement licite. Cette possibilité de blocage prend toute sa signification dans les cas où l'autorité n'est pas à même d'apprécier l'ensemble des

dangers que pourrait faire encourir la communication en fonction d'éléments propres à la situation de la personne concernée.

L'al. 4 prévoit la possibilité de s'opposer à une communication de données déterminées. Par communication de données déterminées, il faut entendre selon les cas soit certaines données, soit une communication spécifique ou en vue d'une finalité spécifique. Il suffit à la personne concernée de rendre vraisemblable un intérêt légitime. Les exigences ne seront pas trop élevées et une pesée d'intérêts sera faite si l'autorité a des raisons d'envisager de rejeter l'opposition au sens de l'al. 5.

L'al. 5 restreint les effets du blocage. L'autorité est légitimée à communiquer les données malgré le blocage lorsqu'elle est juridiquement tenue de le faire ou lorsque le défaut de communication risque de compromettre l'accomplissement de ses tâches légales.

1.16 Article 23

Cet article concerne le cas particulier de la communication de données par le contrôle des habitants lorsqu'elles sont classées de manière systématique. La communication individuelle de données par le contrôle des habitants est régie par l'art. 22 comme pour les autres autorités. L'art. 23 est une *lex specialis* qui déroge à l'art. 22 lorsque les données sont classées de manière systématique. La communication individuelle de données par le contrôle des habitants continue à être régie par l'art. 22.

L'al. 1 prévoit que le contrôle des habitants peut communiquer à une personne, une organisation privée ou à une autorité, sur demande et si le conseil municipal l'y a autorisé, les nom, prénom, sexe, adresse et date de naissance selon un classement systématique. Comme à l'art. 22, le requérant doit fait valoir un intérêt légitime. Il est précisé que les données ne peuvent pas être utilisées à des fins commerciales, un critère plus objectif que la notion précédente qui conditionnait la communication à des fins idéales dignes d'être soutenues. Il s'agit dans tous les cas d'une possibilité et non d'une obligation pour le contrôle des habitants. Les communes sont responsables de leur organisation et doivent déterminer comment elles autorisent la communication.

La communication de données à une autre autorité doit être prévue par une base légale suffisante, en principe la base légale qui fonde les compétences de l'autorité qui demande les données.

La possibilité de s'opposer à cette communication est spécifiquement mentionnée à l'al. 2bis. Aucune forme particulière n'est requise et la personne concernée n'a pas besoin de motiver son opposition. Le contrôle des habitants pourrait proposer un formulaire, mais il ne saurait s'en prévaloir pour refuser de tenir compte d'une opposition exprimée clairement par un autre biais, par exemple par courrier voire oralement au guichet.

Une levée de l'opposition semble peu probable, sauf dans le cas évidemment où une loi prévoit la communication. Au besoin, l'art. 22 al. 5 peut être appliqué par analogie.

1.17 Article 24

La disposition sur la communication de données à des sociétés de services est abrogée. Les conditions classiques de la sous-traitance figurant à l'art. 29 sont suffisantes. Les exigences de solvabilité et de moralité qui se retrouvaient à l'art. 29 se retrouvent en partie dans l'obligation générale à charge du responsable du traitement de choisir avec diligence son sous-traitant (*cura in eligendo*).

1.18 Article 25

L'art. 25 prévoit les conditions auxquelles des données peuvent être communiquées hors de Suisse.

La portée matérielle de l'al. 1 demeure inchangée. Il s'agit simplement de simplifications rédactionnelles.

Au vu de la hiérarchie instituée par le droit fédéral et européen, les garanties appropriées font désormais l'objet d'un alinéa spécifique (al. 2).

Pour être valide, le consentement de la personne concernée doit respecter les critères fixés à l'art. 18 al. 4. L'exigence d'une information claire sur les risques en cas d'absence de protection adéquate est ajoutée, afin de respecter la Convention 108+, même si la nLPD n'a étonnamment pas repris cette exigence.

Lorsque la communication est basée sur la conclusion ou l'exécution d'un contrat (al. 3 let. e), il est précisé que la communication doit non seulement être en relation directe avec le contrat, mais également que ce contrat doit soit lier le responsable du traitement et la personne concernée, soit le responsable du traitement et un tiers pour autant que ce soit dans l'intérêt de la personne concernée. La formulation correspond à celle de l'art. 14 al. 1 let. b nLPD.

Afin de vérifier que les conditions de la communication transfrontière de données sont respectées, le préposé peut exiger des autorités la production de documents.

1.19 Article 26

L'art 26 prévoyait la communication de données sans référence à la personne concernée à des conditions facilitées. Cette exception doit s'appliquer non seulement à la communication, mais à toutes les opérations de traitement. Elle correspond à l'art. 35 nLPD.

L'al. 1 prévoit cinq conditions cumulatives. Premièrement, le but du traitement doit entrer dans un cadre de recherche, planification ou statistique et ne pas se rapporter aux personnes. Deuxièmement, les données sont rendues anonymes dès que la finalité du traitement le permet. Troisièmement, l'autorité ne communique des données sensibles à des personnes privées que sous une forme ne permettant pas

d'identifier la personne concernée. Cette condition est aussi réalisée lorsque les données sont communiquées sous une forme pseudonyme, et que la clé pour réidentifier la personne reste chez celui qui transmet les données (anonymisation factuelle) et que le destinataire n'a pas d'autres moyens de retrouver la clé ou d'identifier les personnes par d'autres moyens. Quatrièmement, le destinataire ne communique les données à des tiers qu'avec le consentement de l'autorité qui les lui a transmises. Cinquièmement, si les résultats du traitement sont publiés, ils doivent l'être sous une forme ne permettant pas d'identifier la personne concernée.

On entend par rendre anonyme, toute démarche visant à empêcher l'identification de la personne concernée ou à ne rendre celle-ci possible qu'au prix d'efforts démesurés. En pratique, il arrive fréquemment que le chercheur, le planificateur ou le statisticien, bien qu'il utilise des données dépourvues de références à des personnes déterminées, n'entende néanmoins pas les rendre d'emblée anonymes, car il doit conserver la possibilité de vérifier exceptionnellement l'identité d'une personne. Lorsqu'il est confronté à de telles situations, il se doit de pseudonymiser les données.

L'al. 2 est complété par un autre principe qui n'a pas besoin d'être respecté en matière de traitement de données sans référence à la personne concernée. Il s'agit de celui de l'exigence de la base légale. Cet ajout est introduit afin d'assouplir les possibilités de traitement de données sans référence à la personne concernée vu que le risque d'atteinte pour ces dernières est plutôt faible.

1.20 Article 28

Les modifications de l'art. 28 sont essentiellement rédactionnelles et n'ont pas de portée matérielle. Les conditions cumulatives prévues à l'al. 2 pour l'installation d'appareils de prises de vue et d'enregistrement d'images sur le domaine public sont gardées. À ce titre, il est primordial que l'autorité adopte une loi au sens formel avant toute installation. La LIPDA n'est pas une base légale suffisante pour autoriser l'installation d'appareils de prises de vue et d'enregistrements d'images sur le domaine public.

1.21 Article 28a

Comme indiqué à l'art. 28 LIPDA, une loi au sens formel est nécessaire pour autoriser l'installation des appareils de prise de vues et d'enregistrement d'images sur le domaine public.

Par le nouvel art. 28 a al. 1 LIPDA, le législateur indique que pour l'espace communal ou intercommunal, la nécessité d'une base légale formelle pour l'installation d'appareils de prise de vues et d'enregistrement d'images à des fins de sécurité publique est remplie par les dispositions contenues dans un règlement communal ou

intercommunal, avalisé par le conseil général ou l'assemblée primaire et homologué par le Conseil d'Etat.

Pour l'espace public cantonal, la nécessité d'une base légale formelle pour l'installation d'appareils de prise de vues et d'enregistrement d'images à des fins de sécurité publique est remplie par la loi sur la police cantonale ainsi que par l'ordonnance sur les mesures de vidéo et d'audio-surveillance par la police cantonale (art. 28a al. 2 LIPDA).

1.22 Article 28b

Conformément à la Directive (UE) 2016/680, une nouvelle disposition contenant des obligations générales pour le responsable du traitement et le sous-traitant est ajoutée. Ils doivent être en mesure de démontrer en tout temps leur conformité à la loi et prendre toutes les mesures appropriées pour s'assurer de cette conformité. Cela correspond également au principe de responsabilité (*compliance*) figurant à l'art. 5 par. 2 RGPD. Afin de s'assurer de sa conformité et d'être en mesure de le démontrer, ils doivent mettre en œuvre des mesures techniques et organisationnelles appropriées, qui doivent être réexaminées et actualisées si nécessaire.

L'al. 2 concerne les situations où plus d'une autorité est responsable du traitement. Les responsables conjoints du traitement doivent se mettre d'accord notamment en ce qui concerne l'exercice des droits de la personne concernée et leurs obligations respectives quant à la communication des informations à mettre à la disposition ou à fournir à la personne concernée. Le point de contact pour la personne concernée est mentionné dans l'accord et la personne concernée doit savoir quelle responsabilité est assumée par quelle autorité.

1.23 Article 29

L'art. 29 est reformulé et complété afin de poser les règles à respecter en cas de sous-traitance (parfois aussi appelé délégation de traitement). Il s'inspire de l'art. 8 nLPD.

L'al. 1 précise que la sous-traitance est admise si trois conditions sont remplies. Premièrement, elle est prévue dans un contrat ou dans la loi. Deuxièmement, le sous-traitant est limité par les instructions du responsable du traitement et ne peut effectuer que les traitements qui sont permis au responsable du traitement. Dans ce cadre, le sous-traitant peut faire valoir les mêmes motifs justificatifs que le responsable du traitement (al. 5). Troisièmement, aucune obligation légale ou contractuelle de garder le secret n'interdit la sous-traitance. On pense ici en particulier au secret de fonction. Cela ne signifie pas qu'une sous-traitance est interdite lorsque des données sont protégées par un secret, mais elle devra respecter intégralement les exigences dudit secret pour être licite au sens de l'art. 29.

L'al. 2 exige un contrat écrit, contrairement à l'art. 8 nLPD qui n'en précise pas la forme. Cela implique une signature manuscrite ou qualifiée au sens de l'art. 14 CO. Un contrat de sous-traitance oral serait source de risques importants, raison pour laquelle il est exclu. Il est précisé que la forme électronique est également acceptée. Les éléments essentiels devant figurer dans le contrat sont énumérés à l'al. 2, conformément à ce qui est prévu dans le RGPD et dans la Directive (UE) 2016/680. Le préposé peut proposer un modèle de contrat pour faciliter la tâche des autorités.
Le responsable du traitement reste responsable des traitements qu'il a délégués au sous-traitant. L'obligation pour le responsable du traitement qui charge un tiers d'exécuter un traitement de données de veiller à ce que la protection de ces informations et du résultat du traitement soit garantie conformément à la présente loi est reprise de manière plus détaillée à l'al. 3.
L'al. 4 prévoit que la sous-traitance de deuxième rang n'est possible que sur la base d'une autorisation écrite préalable du responsable du traitement. Il s'agit du cas où le sous-traitant désigné par le responsable du traitement désire lui aussi déléguer tout ou partie du traitement des données à un tiers. L'autorisation peut être donnée de manière générale ou spécifique à la conclusion du contrat de sous-traitance, ou à l'ajout de chaque nouveau sous-traitant. Dans la mesure du possible cette seconde manière de faire doit être préférée.
L'al. 6 impose au sous-traitant de tenir un registre contenant des informations relatives aux traitements effectués pour le compte du responsable du traitement. Il ne doit pas être confondu avec le registre public prévu à l'art. 30. Le registre du sous-traitant doit permettre au responsable du traitement et à l'autorité de surveillance d'avoir accès à toutes les informations nécessaires pour vérifier que le sous-traitant respecte ses obligations en matière de protection des données.

1.24 Article 30

L'obligation pour chaque autorité de tenir son propre registre des fichiers et d'informer le préposé lorsqu'il contient des données sensibles est remplacée par une obligation de déclarer les traitements au préposé comme cela est prévu à l'art. 11 al. 4 nLPD. Puisqu'il n'y a plus qu'un registre cantonal, le titre de l'art. 30 est adapté en conséquence.
Concrètement, le registre est tenu par le préposé qui en assure le bon fonctionnement technique et sa publicité. Le recours à un seul registre facilite l'accès à l'information puisque le justiciable n'a plus qu'un seul registre à consulter pour toutes les autorités. Chaque autorité reste néanmoins seule responsable du contenu du registre qu'elle doit compléter pour les traitements qu'elle effectue. Cette obligation ne s'applique pas

aux sous-traitants, qui doivent certes tenir un registre conformément à l'art. 29 al. 6, mais qui ne correspond pas au registre public dont il est question ici.

Le principe figure à l'al. 1 et le contenu du registre à l'al. 2. Il doit au moins contenir pour chaque activité de traitement des informations sur l'autorité responsable du traitement et une personne de contact, la base légale, les finalités, les personnes concernées ou les catégories de personnes concernées, les données ou au moins les catégories de données, le cas échéant les destinataires prévus, la durée de conservation ou au moins les critères pour la déterminer, ainsi que les mesures visant à garantir la sécurité.

L'al. 3 permet au Conseil d'Etat de prévoir des exceptions à l'obligation d'enregistrer certaines activités de traitement. Il n'est donc pas nécessaire de prévoir des exceptions spécifiques dans la loi. On peut imaginer ici un traitement très ponctuel ou par une autorité disposant de moyens limités et portant sur un nombre restreint de personnes, pour autant que les traitements en question ne représentent pas de risque pour la personne concernée. L'exception relative aux traitements qui servent exclusivement à l'accomplissement de tâches de l'administration et ne déploient pas d'effets externes est déplacée dans le règlement. Ce qui n'est pas le cas de l'exception relative aux traitements qui seraient régulièrement publiés, qui est supprimée, sans quoi le risque de perdre l'intérêt d'un registre unique est trop important. Le Conseil d'Etat peut aussi prévoir une déclaration simplifiée plutôt que l'exemption complète. La règle doit néanmoins rester la déclaration.

1.25 Article 30a

L'art. 30a introduit une obligation d'annoncer toute violation de la sécurité des données comme cela est prévu à l'art. 22 nLPD et par les textes de droit européen.

L'al. 1 dispose que le responsable du traitement annonce au préposé dans les meilleurs délais toute violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

La notion de « violation de la sécurité des données » est définie à l'art. 3 et recouvre toute violation de la sécurité, sans égard au fait qu'elle soit intentionnelle ou illicite, entraînant la perte de données à caractère personnel, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données. La violation peut être causée par un tiers, mais son auteur peut aussi être un employé qui outrepasse ses compétences ou qui fait preuve de négligence. La violation de la sécurité des données peut entraîner une perte de contrôle de la personne concernée sur ses données ou une utilisation abusive de celles-ci. Elle peut

aussi engendrer une violation de la personnalité, par exemple en entraînant la divulgation d'informations que la personne souhaitait garder secrètes.

L'atteinte à la sécurité des données est une violation de la personnalité. La personne concernée ne peut réagir à ces menaces que si elle sait que la sécurité des données a été violée. C'est pourquoi le responsable du traitement doit annoncer tout traitement non autorisé au préposé en premier lieu et, si les conditions de l'al. 4 sont remplies, à la personne concernée également.

L'annonce doit avoir lieu dans les meilleurs délais à partir du moment où le traitement non autorisé est connu. Le responsable du traitement doit agir rapidement, en principe dans les trois jours, mais la disposition lui laisse une certaine marge d'appréciation, qui dépend en pratique de l'ampleur du risque pour la personne concernée. Plus ce risque est élevé et le nombre de personnes concernées important, plus son intervention doit être rapide.

Toutes les violations de la sécurité des données ne justifient pas une annonce. Au contraire, c'est seulement s'il est vraisemblable que la violation de la sécurité des données entraînera un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée qu'une annonce est nécessaire. Il s'agit d'éviter l'annonce de violations insignifiantes. La perte temporaire de données chiffrées, sans que la clé de déchiffrement n'ait été exposée ni ne risque d'avoir été découverte, ou l'accès à des données publiquement accessibles par un autre biais, ne nécessitent en principe pas d'annonce.

Le responsable du traitement doit évaluer dans tous les cas les conséquences possibles de la violation pour la personne concernée et documenter la raison pour laquelle il considère que la violation n'a pas à être signalée.

L'al. 2 précise les indications que l'annonce au préposé doit contenir au minimum. Le responsable du traitement doit tout d'abord indiquer la nature de la violation, pour autant que cela lui soit possible. On distingue quatre types de violations : l'effacement ou la destruction de données, leur perte, leur modification ou leur communication à des tiers non autorisés. L'annonce doit aussi expliquer, dans la mesure du possible, les conséquences de la violation de la sécurité des données. Ce sont avant tout les conséquences pour la personne concernée et non les conséquences pour le responsable du traitement qui sont envisagées. Enfin, il y a lieu de préciser également les mesures prises ou envisagées pour remédier à la violation de la sécurité des données ou pour atténuer ses conséquences. L'annonce doit permettre dans tous les cas au préposé d'intervenir le plus rapidement et le plus efficacement possible. Si toutes les informations ne sont pas immédiatement disponibles, le responsable du

traitement ne doit pas différer l'annonce, mais au contraire communiquer sans délai les informations dont il dispose et les compléter ou les rectifier par la suite.
Pour faciliter la communication des informations, le préposé peut prévoir un formulaire-type ou une communication en ligne sécurisée.
L'al. 3 vise le cas où la violation de la sécurité des données se produit chez le sous-traitant. Il doit alors informer le responsable du traitement dans les meilleurs délais de tout traitement non autorisé. C'est ensuite au responsable du traitement de procéder à une évaluation des risques et de décider si une notification au préposé et à la personne concernée s'impose. Le sous-traitant doit informer de toute violation de la sécurité des données, et pas seulement celle qui nécessite une communication. Même si la loi prévoit cette obligation, il est recommandé de le mentionner expressément dans les contrats de sous-traitance.
L'al. 4 prévoit une information de la personne concernée dans deux cas particuliers, soit si les circonstances le requièrent ou si le préposé l'exige. Le premier cas vise en particulier les situations où l'information des personnes concernées peut leur permettre de prendre des mesures pour réduire les risques pour leur personnalité ou leurs droits fondamentaux, par exemple en modifiant des données d'accès ou du mot de passe, ou encore parce qu'il existe un risque important que les informations soient rendues publiquement accessibles. Le deuxième cas doit permettre au préposé d'exiger la communication aux personnes concernées soit parce qu'il considère, contrairement au responsable du traitement, qu'elles pourraient prendre des mesures ou simplement parce qu'il y a un autre intérêt important à les informer.
La communication doit avoir lieu par écrit (courrier postal ou courrier électronique selon les circonstances). Si la communication aux personnes concernées seulement n'est pas possible ou rendue trop difficile, par exemple parce qu'il n'est pas (encore) possible de les identifier précisément, une communication à un nombre plus large de personnes peut être admise si au moins les personnes concernées sont informées. Dans des cas particuliers, on pourrait admettre également une communication publique plutôt qu'une information individuelle comme le prévoit l'al. 5 let. c.
L'al. 5 dispose que le responsable du traitement peut, dans certains cas, restreindre l'information de la personne concernée, la différer ou y renoncer. Cela ne concerne pas l'annonce au préposé. Dans la mesure du possible, il est toujours préférable de différer une annonce plutôt que d'y renoncer.
La let. a vise le cas où un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de l'Etat, s'oppose à l'information, ou si elle est susceptible de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative.

La let. b admet aussi une restriction de l'information s'il n'est pas possible de respecter le devoir d'informer ou si l'information nécessiterait des efforts disproportionnés. Le devoir d'informer est réputé impossible à respecter lorsque le responsable du traitement n'est pas en mesure d'identifier les personnes concernées par la violation de la sécurité des données, par exemple parce que les fichiers journaux qui permettraient une identification ne sont plus disponibles. On estime de même que l'information nécessite des efforts disproportionnés dès lors qu'il faudrait informer individuellement un grand nombre de personnes concernées et que les coûts qui en résulteraient semblent excessifs au regard du gain qu'en retireraient les personnes concernées. Cette exception ne devrait pas s'appliquer si les personnes concernées peuvent prendre des mesures utiles ou si une communication publique au sens de la let. c'est envisageable.

La let. c autorise précisément le responsable du traitement à opter pour une communication publique si l'information des personnes concernées est garantie de manière équivalente. On estime que cette condition est remplie quand une annonce individuelle ne permettrait pas d'améliorer sensiblement l'information de la personne concernée et que les personnes concernées ont accès à l'information publique.

La let. d oblige le responsable du traitement à tenir compte des intérêts d'un tiers lorsque ces derniers sont prépondérants par rapport à l'information de la personne concernée. Pour se prévaloir de cette exception, le responsable du traitement doit procéder à une pesée des intérêts. L'information ne peut être restreinte au motif que l'intérêt d'un tiers serait prépondérant que dans des cas limités.

1.26 Article 30b

L'obligation de procéder à une analyse d'impact relative à la protection des données à caractère personnel concrétise les exigences du droit européen et s'aligne sur les art. 20 et 21 nLPD. Conformément au principe de protection des données dès la conception, il s'agit d'un instrument destiné à identifier et à évaluer en amont les risques que certains traitements pourraient entraîner. Cet instrument étant nouveau, le préposé devra guider les autorités, notamment en fournissant des critères et des exemples de traitement qui représentent ou non un risque élevé, ou un document type pour faciliter l'établissement de l'analyse d'impact. En l'absence, les autorités pourront aussi s'inspirer de la méthode de gestion de projets Hermès largement utilisée au niveau fédéral.

L'al. 1 prévoit que le responsable du traitement procède à une analyse d'impact lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Il peut effectuer une analyse d'impact commune s'il envisage d'effectuer plusieurs opérations de

traitement semblables (objectif commun). Il n'est alors pas nécessaire d'examiner individuellement chacune des étapes prévues pour chaque opération, mais l'analyse peut porter sur l'ensemble des opérations.

Le responsable du traitement est donc tenu de faire un pronostic des conséquences que le traitement en question peut avoir pour la personne concernée. Sont déterminantes, notamment, la nature et l'ampleur de l'impact du traitement sur la personnalité ou les droits fondamentaux de la personne concernée.

L'al. 2 précise que l'existence d'un risque élevé dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Plus le traitement est étendu, plus il y a de données sensibles et plus la finalité du traitement est vaste, plus il y a lieu de conclure à un risque élevé. Un tel risque existe par exemple s'il y a un traitement d'un grand volume de données sensibles comme cela peut se produire dans le cadre de projets de recherche médicaux (let. a), en cas de profilage (let. b) ou en cas de surveillance de grandes parties du domaine public (let. c).

Pour évaluer s'il est face à un risque élevé, le responsable du traitement peut s'inspirer des neufs critères de risques retenus par le Groupe de travail art. 29[8], soit : évaluation ou notation (y compris les activités de profilage et de prédiction), prise de décisions automatisée avec effet juridique ou effet similaire significatif, surveillance systématique, données sensibles ou données à caractère hautement personnel, données traitées à grande échelle (nombre de personnes concernées, volume de données, durée et étendue géographique de l'activité de traitement), croisement ou combinaison d'ensembles de données, données concernant des personnes vulnérables, utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles, traitements en eux-mêmes qui empêchent la personne concernée d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

L'al. 3 précise le contenu de l'analyse d'impact relative à la protection des données. Elle doit tout d'abord décrire le traitement envisagé (processus, technologies employées, finalité, durée de conservation des données), puis montrer quels risques le traitement implique pour la personnalité ou les droits fondamentaux de la personne concernée. Il s'agit ici d'un approfondissement de l'évaluation des risques qui doit déjà être faite en amont, lors de l'examen de la nécessité de procéder à une analyse d'impact. Il convient ainsi de présenter la nature du risque élevé qu'engendre le traitement envisagé et les moyens de l'évaluer. L'analyse d'impact doit ensuite expliquer les mesures prévues pour faire face à ce risque (pseudonymisation,

[8] Groupe de travail art. 29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 adoptées le 4 avril 2017 et révisées le 4 octobre 2017 (WP 248 rév. 01), p. 4.

minimisation, mesures de sécurité particulières, protection des données dès la conception et par défaut) et les risques résiduels. Finalement, il est encore possible de mettre en balance les intérêts de la personne concernée et ceux du responsable du traitement.

L'al. 4 prévoit que le responsable du traitement doit informer le préposé préalablement au traitement s'il ressort de l'analyse d'impact que le traitement envisagé présente un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée malgré les mesures envisagées. Cette obligation est plus limitée que celle prévue dans le RGPD ou la LPDS et qui exige de consulter le préposé chaque fois que le traitement présenterait un risque élevé si l'organe fédéral ne prenait pas de mesures pour atténuer ce risque.

L'information du préposé doit lui permettre d'exercer sa fonction de conseil et de prévention. Il dispose alors d'un délai de deux mois pour formuler des objections concernant le traitement envisagé et proposer des mesures appropriées. Lorsqu'il est informé du résultat d'une analyse d'impact, le préposé vérifie si les mesures proposées sont suffisantes pour protéger la personnalité et les droits fondamentaux de la personne concernée. S'il arrive à la conclusion que le traitement contreviendrait, dans la forme envisagée, aux dispositions de la LIPDA, il propose des mesures appropriées au responsable du traitement. Si le responsable ne reçoit pas de nouvelles du préposé dans le délai de deux mois, il peut partir du principe que le préposé n'a pas d'objections contre les mesures envisagées.

Le préposé n'en reste pas moins libre d'ouvrir une enquête ultérieurement si les conditions de l'art. 37 sont remplies, en particulier s'il apparaît que les risques n'ont pas été correctement évalués dans le cadre de l'analyse d'impact et que, par conséquent, les mesures définies ratent leur cible ou sont insuffisantes.

1.27 Article 30c

Chaque autorité soumise à la LIPDA doit désigner un délégué à la protection des données. Le terme de délégué à la protection des données a été retenu conformément à la Directive (UE) 2016/680, même si la nLPD et la LPDS parlent de conseiller à la protection des données. Il ne s'agit que d'une différence terminologique.

Le délégué à la protection des données est le point de contact privilégié pour les personnes concernées et pour les autorités de surveillance en matière de protection des données. Il veille au respect des prescriptions de protection des données au sein d'une autorité et prodigue au responsable du traitement des conseils en matière de protection des données. Le responsable du traitement reste cependant le seul responsable en cas de violations des prescriptions légales.

Un collaborateur ou un tiers peut être nommé. Le délégué doit cependant exercer sa fonction de manière indépendante et sans recevoir d'instructions du responsable du traitement afin de pouvoir exercer correctement ses tâches de conseil. Dans le cas où l'autorité choisit de recourir aux services d'un tiers, elle doit le faire par le biais d'un contrat de mandat.

L'al. 2 let. a impose au délégué d'avoir les connaissances professionnelles nécessaires pour exercer ses tâches. Les connaissances doivent notamment porter sur la législation en matière de protection des données et sur les normes techniques relatives à la sécurité des données.

L'autre condition à remplir (al. 2 let. b) est l'interdiction d'exercer des tâches incompatibles avec sa mission. Il ne doit par exemple pas avoir de rôle dans les domaines de la conduite du personnel ou de la gestion des systèmes informatiques.

1.28 Article 31

Cet article est complété afin de clarifier le déroulement des demandes d'accès aux données à caractère personnel. Il reprend en partie le contenu des anciens art. 48 et 51, en ne prenant en compte toutefois que la question de l'accès aux données à caractère personnel. L'accès aux documents officiels est traité dans le chapitre correspondant.

L'al. 1 prévoit désormais non seulement le droit de demander, mais surtout le droit de recevoir (sous réserve des exceptions prévues à l'art. 32) la confirmation d'un traitement et un certain nombre d'informations y relatives.

L'accès aux données implique le droit pour la personne concernée de connaître l'identité et les coordonnées du responsable du traitement ; la base légale et les finalités du traitement ; quelles sont les données traitées ; toute information disponible sur leur origine ; les destinataires ou les catégories de destinataires ; la durée de conservation ou au moins les critères pour la déterminer ; ainsi que l'existence d'une décision individuelle automatisée et la logique sur laquelle elle se base.

Le responsable du traitement est libre de décider s'il préfère indiquer les destinataires ou les catégories de destinataires. Si le responsable du traitement ne souhaite pas révéler l'identité des destinataires, il peut se contenter d'indiquer leur catégorie. Les sous-traitants font partie des destinataires.

S'il n'est pas possible de communiquer la durée de conservation des données, le responsable du traitement peut indiquer les critères retenus pour la fixer.

Une information préalable relative à l'existence d'une décision individuelle automatisée doit être faite (art. 20). Il n'est pas exigé d'expliquer en amont la logique sur laquelle cette décision se base. En revanche, en cas de demande d'accès, non seulement l'existence, mais également la base de cette décision doit être

communiquée (art. 31 al. 1 let. h). Il n'y a alors pas lieu de révéler à la personne les algorithmes utilisés, qui relèvent souvent du secret d'affaires, mais plutôt les hypothèses de base qui sous-tendent la logique algorithmique sur laquelle repose la décision individuelle automatisée. Par exemple, des détails peuvent être donnés sur les caractéristiques principales prises en compte pour la prise de décision, la source des informations et leur pertinence, ainsi que sur les tests effectués pour s'assurer que les décisions restent justes, efficaces et impartiales.

Les al. 3 et 4 concernant les questions de forme sont repris de l'ancien art. 48 al. 1 et 3. L'al. 5 introduit dans la loi le délai prévu précédemment dans le règlement d'exécution. L'al. 6 est introduit afin d'uniformiser le traitement de la demande d'accès à des données avec la demande d'accès aux documents officiels (art. 12b al. 2).

Quant à l'al. 7, il est repris pour l'essentiel de l'ancien art. 51. Un tiers est notamment concerné dès lors que des données à caractère personnel le concernant peuvent être révélés dans le cadre d'une demande de droit d'accès. Cet accès doit encore porter atteinte à la personnalité du tiers. Le caviardage des données à caractère personnel du tiers est à privilégier.

1.29 Article 32

Seule la question de la restriction au droit d'accès est traitée ici. Le titre de l'article est donc adapté en conséquence.

Une restriction au droit d'accès est possible lorsqu'il s'agit d'une mesure nécessaire et proportionnée pour éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires, pour éviter de nuire à la prévention ou la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales, et pour protéger la sécurité publique, les droits et les libertés d'autrui. La communication de renseignements ou le droit de consultation peut aussi être différé même si la loi ne le prévoit pas expressément.

Un al. 2 est ajouté pour préciser qu'une limitation ou un refus d'accès doit être motivé par le responsable du traitement. Ceci afin de permettre à la personne concernée de comprendre et, cas échéant, de contester la limitation ou le refus. Bien entendu, la limitation ou le refus d'accès peut être temporaire. Un renforcement des droits des personnes concernées est un des éléments importants des développements récents en matière de protection des données, que ce soit au niveau européen ou fédéral. Les voies de droit sont prévues par l'art. 52.

1.30 Article 33

La personne concernée a non seulement un droit d'accès à ses données, mais également le droit de les faire rectifier ou détruire lorsqu'elles sont incorrectes. Le droit d'accès seul ne serait pas d'une grande utilité pratique si son but n'était pas de

permettre à la personne concernée de vérifier les traitements effectués sur ses données et de pouvoir les contester, ainsi que les données en tant que telles.
Les modifications de l'al. 1 sont essentiellement rédactionnelles et n'ont pas de portée matérielle. L'al. 2 est inchangé.
L'al. 3 est modifié de telle sorte que lorsque le responsable du traitement ne peut pas apporter la preuve immédiate de l'exactitude des données contestées, la personne concernée peut exiger la mention du caractère contesté des données et de l'opposition au sens de l'art. 22 al. 4. La notion de suppression provisoire de l'ancien al. 3 est supprimée.
La possibilité de ne pas effacer ou détruire les données mais uniquement de limiter le traitement est offerte au responsable du traitement dans certains cas, qui sont énumérés à l'al. 3bis let. a à d.
En outre, un nouvel al. 3ter prévoit que lorsque des données inexactes ont été transmises ou lorsqu'il y a transmission illicite, le responsable du traitement a l'obligation d'en informer le destinataire sans délai. Le destinataire doit alors rectifier ou supprimer les données en question. L'obligation n'est pas sans limite mais l'autorité doit néanmoins faire un effort raisonnable pour identifier et informer les destinataires.
L'al. 3quater introduit la possibilité pour le responsable du traitement de ne pas donner suite aux droits de l'al. 1 lorsqu'il existe des motifs légitimes justifiant le traitement qui prévalent sur les intérêts ou les droits et libertés fondamentales de la personne concernée.

1.31 Article 34

L'opposition à la communication, qui correspond à l'ancienne notion de blocage, figure désormais à l'art. 22 al. 4 et 5. Elle est complétée par un droit plus général de s'opposer à tout traitement de données, conformément à dans l'art. 9 par. 1 let. d de la Convention 108+. En conséquence, le titre marginal ainsi que le contenu de l'art. 34 sont totalement modifiés.
L'art. 34 prévoit que la personne concernée qui rend vraisemblable un intérêt digne de protection peut s'opposer à tout moment à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. Il appartient à la personne concernée de rendre vraisemblable un intérêt digne de protection à l'appui de son droit d'opposition.
Immédiatement après la réception d'une demande d'exercice du droit d'opposition, le responsable du traitement doit restreindre le traitement pendant la vérification portant sur le point de savoir si l'intérêt digne de protection évoqué par la personne concernée prévaut sur la continuation du traitement. La personne concernée doit être informée

de la décision du responsable du traitement, qui, en cas de refus, doit être en mesure de démontrer qu'il n'existe aucun intérêt digne de protection.

La demande d'opposition à un traitement n'est soumise à aucune exigence de forme.

1.32 Article 35

De manière générale, le statut et le rôle de l'autorité de surveillance devaient être repensés pour renforcer son indépendance et lui donner la possibilité de rendre des décisions contraignantes à l'égard des responsables du traitement, au terme d'une enquête ouverte d'office ou sur dénonciation.

C'est ainsi une structure bipartite qui est conservée, composée d'un préposé à la protection des données et à la transparence (le préposé) et d'une commission cantonale de protection des données et de transparence (la commission). Une telle structure est courante dans les cantons latins. Elle se distingue du modèle fédéral qui ne connaît pas de commission de protection des données. Contrairement à ce qui prévalait précédemment, et s'inspirant du modèle jurassien et neuchâtelois, les deux autorités sont désormais indépendantes. Il fallait d'une part simplifier les procédures, et d'autre part garantir que le préposé puisse jouer son rôle de conseil et de médiateur. S'il fait partie, est rattaché ou dépend, de l'autorité décisionnelle (la commission), le préposé perd l'indépendance requise pour conseiller les autorités. La taille du canton ne permet pas non plus d'avoir suffisamment de personnes au sein du bureau du préposé pour que certaines s'occupent de la partie conseil et d'autres rendent des décisions comme c'est imaginable au niveau fédéral. Le titre 4 est adapté en conséquence. Le préposé a principalement des tâches de conseil et de médiation, alors que la commission est l'autorité de décision de première instance. La commission est une autorité judiciaire indépendante et non un organe politique. Ces deux autorités continueront d'exercer aussi la surveillance dans les communes.

L'al. 2 prévoit que le préposé, ainsi que le président et les membres de la commission, sont nommés par le Grand Conseil. Ce mode d'élection s'aligne sur ce qui est prévu dans la nLPD (art. 39) et doit aussi assurer l'indépendance de l'autorité de surveillance vis-à-vis du Conseil d'Etat et de l'administration. Il s'agit d'une nomination et les détails de la fonction doivent être réglés dans la LIPDA, éventuellement le RELIPDA, mais pas dans un mandat de droit privé.

Le préposé, ainsi que le président et les membres de la commission sont évidemment soumis au secret de fonction. Le secret couvre toute information confidentielle dont ils ont eu connaissance dans l'exercice de leurs missions et de leurs pouvoirs, y compris après la cessation de leurs activités. Ce devoir s'applique également au signalement par des personnes physiques de violations de la présente loi.

Le préposé, ainsi que le président et les membres de la commission exercent leurs fonctions de manière indépendante et impartiale. Les autorités de surveillance doivent bénéficier d'une indépendance du point de vue fonctionnel, institutionnel, personnel et matériel[9]. L'al. 3 précise qu'ils ne doivent ni recevoir ni solliciter d'instructions de la part d'une autorité ou d'un tiers. Ils doivent être libres de toute influence extérieure, qu'elle soit directe ou indirecte. L'indépendance s'applique aussi entre les deux organes qui s'acquittent de leur tâche de manière autonome. Le préposé ne fait pas partie de la commission ni n'en reçoit d'instructions. Cela doit lui assurer une marge de manœuvre suffisante et éviter les problèmes de récusation, ainsi qu'une approche plus pragmatique, souple et proche du citoyen, telle que celle pratiquée dans les différents cantons suisses. Les autorités sont tenues à collaborer avec le préposé et la commission.

Conséquence de leur autonomie et leur indépendance, ils doivent disposer à cette fin des moyens nécessaires et, en particulier, disposer chacun de leur propre budget. Ils remettront d'ailleurs chaque année, par l'intermédiaire du service parlementaire, leur projet de budget au Grand Conseil (al. 4). Tant le préposé que la commission sont soumis à l'Inspectorat cantonal des finances.

L'al. 5 impose tant au préposé qu'à la commission de faire annuellement un rapport écrit de leurs activités. Le rapport doit être remis jusqu'au 31 mars. Il est adressé au Conseil d'Etat et au Grand Conseil, ainsi que rendu public. C'est un outil important non seulement pour contrôler l'activité de l'autorité de surveillance, mais surtout pour participer à la sensibilisation des autorités et du public. Le rapport peut comprendre une liste des types de violations notifiées et des types de sanctions imposées.

1.33 Article 36

L'al. 1 précise la durée du mandat du préposé qui est maintenue à quatre ans. Le renouvellement est limité et la durée totale ne doit pas excéder trois mandats (douze ans au maximum). La période de fonction du préposé débute le 1er janvier suivant le début de la législature du Grand Conseil.

Dans l'ancienne loi, la période de fonction du préposé n'est pas limitée. Ce principe est modifié pour s'aligner sur la nLPD et le droit européen. Cette mesure permet de renforcer l'indépendance du préposé en tant qu'autorité. Sachant que son mandat est limité, la crainte de ne pas être reconduit dans sa fonction est limitée et ne devrait pas constituer un frein à l'accomplissement de ses tâches.

[9] Voir notamment « L'indépendance de l'autorité cantonale de surveillance en matière de protection des données », Avis de droit réalisé sur mandat de la Direction de la Sécurité et de la Justice du Canton de Fribourg par Bernhard Waldmann et André Spielmann, Février 2010.

Le préposé peut demander à être libéré de ses fonctions avec un préavis de six mois. Dans le cas d'une démission intervenant moins de 6 mois avant la nouvelle législature, une personne peut être exceptionnellement désignée par intérim sur la base de l'art. 36a. Afin d'assurer son indépendance, il est précisé à l'al. 2 qu'il peut être relevé de ses fonctions que dans des cas très limités, soit s'il est durablement incapable d'exercer ses tâches ou s'il a commis une faute grave dans l'exercice de ses fonctions, par exemple une infraction pénale liée à son activité ou de nature à mettre en doute sa crédibilité. La décision de relever le préposé de ses fonctions est prise par le Grand Conseil en tant qu'autorité de nomination sur préavis de la commission. Les possibilités de relever le préposé doivent être interprétées de manière très restrictive et elles ne doivent en aucun cas être utilisées pour l'empêcher d'exécuter ses tâches légales.

L'al. 3 précise que le préposé dispose d'un secrétariat permanent et qu'il engage son personnel. Son budget est garanti par l'art. 35 al. 3. Le budget doit prendre en compte l'ensemble des charges (salaires, charges sociales, loyers, bibliothèque et matériel informatique, formation continue, mandats tiers, etc.). Le préposé est rattaché administrativement au service parlementaire. Ce dernier ne dispose d'aucun pouvoir d'instructions sur le préposé. Il s'agit d'un attachement purement administratif qui ne remet pas en cause l'indépendance du préposé.

L'al. 4 pose le principe que le préposé ne peut pas exercer une activité accessoire lucrative, ni exercer une fonction au service de la Confédération ou d'un canton, ni être membre de la direction, du conseil d'administration, de l'organe de surveillance ou de l'organe de révision d'une entreprise commerciale, ceci indépendamment de la question de savoir si son activité est rémunérée ou non. Il ne peut donc pas non plus siéger au Conseil d'Etat ou au Grand Conseil. La notion de « canton » doit être comprise dans un sens large, à savoir qu'elle vise également les communes, districts, cercles et corporations de droit public. Sous réserve d'un conflit d'intérêts, son personnel n'est pas soumis à l'interdiction d'exercer une activité accessoire.

Exceptionnellement, le Bureau du Grand Conseil peut autoriser le préposé à exercer une activité accessoire, pour autant que l'exercice de sa fonction ainsi que son indépendance et sa réputation n'en soient pas affectés. Cela pourrait concerner par exemple une activité académique limitée. Sa décision doit être publiée au bulletin officiel.

L'al. 4 ne s'applique pas à la commission. Elle est néanmoins tenue de veiller à l'absence de conflit d'intérêt.

L'al. 5 précise que les écrits et autres documents du préposé produits dans le cadre de son activité appartiennent à l'Etat.

1.34. Article 36a

Cette nouvelle disposition porte sur l'empêchement durable et ponctuel du préposé.

L'al. 1 prévoit qu'en cas d'empêchement durable du préposé, et sur préavis de la commission, le Bureau du Grand Conseil peut désigner un préposé par intérim. Le préposé par intérim est désigné aussi longtemps que dure l'empêchement.

L'al. 2 prévoit qu'en cas d'empêchement ponctuel du préposé, le Bureau du Grand Conseil peut, sur préavis de la commission désigner une personne pour remplir cette fonction *ad hoc*.

Dans les deux cas, le préavis de la commission ne porte que sur l'empêchement du préposé.

1.35 Article 37

Le préposé a essentiellement des tâches de conseil, sensibilisation et médiation. Il peut aussi émettre des recommandations et faire usage de son droit large de saisir la commission, voire de recourir contre les décisions de celle-ci.

L'al. 1 est ainsi complété pour qu'il puisse ouvrir une enquête contre une autorité si des indices font penser qu'un traitement pourrait être contraire à des dispositions en matière de protection des données (let. a). Le préposé peut agir d'office ou sur la base d'une dénonciation, ce qui est également couvert par la let. c. Le préposé peut également saisir la Commission en tout temps pour décision à laquelle des sanctions peuvent être assorties conformément à l'art. 292 CP (let. d) et exercer son droit de recours comme prévu à l'art. 53 (let. e). La let. c est complétée pour que le préposé puisse non seulement traiter une dénonciation, mais également informer l'auteur de la dénonciation des suites données à la dénonciation et du résultat d'une éventuelle enquête. Le dénonciateur n'a pas la qualité de partie. La let. f est également complétée pour que le préposé puisse non seulement approuver les garanties au sens de l'art. 25 al. 3, mais de manière générale vérifier que les communications transfrontières de données se fassent dans le respect du cadre légal. Bien que la let. b ne soit pas modifiée, il sied de préciser que le travail de conseil du préposé implique la sensibilisation du public à la protection des données comme l'exige l'art. 15 par. 2 let. e de la Convention 108+.

Il doit aussi proposer des mesures appropriées lorsqu'il est consulté en cas d'analyse d'impact relative à la protection des données révélant que le traitement présenterait un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (let. j).

Dans le cadre de son activité de conseil, le préposé doit donner son avis sur les projets législatifs touchant à la protection des données et au principe de la transparence ou dans d'autres cas prévus par la loi (let. h). Cela implique que tout

projet de loi concerné lui soit transmis. Il peut évidemment aussi s'exprimer sur un projet de loi sans y avoir été formellement invité.

Suite à l'introduction d'un registre des activités de traitement au niveau cantonal et de l'obligation d'annonce de violations de la sécurité des données, c'est au préposé qu'il revient de tenir ces registres conformément aux art. 30 et 30a (let. i).

Il est aussi rappelé que le préposé doit publier son rapport d'activité conformément à l'art. 35 al. 4 (let. l).

Le préposé est non seulement habilité, mais aussi tenu d'intervenir d'office, pour veiller au respect de la présente loi. A ce titre, il dispose d'un pouvoir d'investigation complet. L'al. 2 prévoit qu'il peut exiger la production de pièces, demander des renseignements et se faire présenter des traitements. Les autorités concernées sont tenues de collaborer à l'établissement des faits. Il peut en particulier, après prise de contact avec le responsable hiérarchique de l'autorité contrôlée, accéder à tous les renseignements, documents, registres et données nécessaires, accéder aux locaux et aux installations auditionner des témoins et ordonner des expertises. En d'autres termes, il peut accéder en tout temps aux locaux où se trouvent des fichiers, se faire présenter ces derniers et les traitements de données, interroger le personnel, ainsi que demander des renseignements et des pièces. Dans ce cadre, le secret de fonction ne peut pas lui être opposé.

L'al. 4 qui prévoyait l'obligation de faire rapport à la commission est supprimé pour garantir l'indépendance de ces deux autorités.

1.36 Article 37a

Cette disposition porte sur l'indépendance et l'organisation du préposé En particulier, le préposé ne reçoit d'instruction d'aucune autorité ou de tiers (al. 1) et s'organise librement (al. 2). Pour ce faire, il doit disposer de locaux permanents mis à disposition par l'État du Valais.

Tant le préposé que ses collaborateurs sont soumis à la Loi sur le personnel de l'État du Valais (al. 3). Le préposé n'est toutefois pas soumis au système de controlling du personnel afin d'éviter toute atteinte à sonindépendance (al. 4).

1.37. Article 37b

La collaboration entre les autorités cantonales, fédérales et étrangère chargées de la protection des données est prévue à l'art. 37b.

Le principe est posé à l'al. 1. Les al. 2 à 4 reprennent dans une large mesure le contenu de l'art. 26 LPDS relatif à l'assistance administrative entre le préposé et les autorités étrangères. Les conditions prévues ne devraient pas poser de problème s'agissant de la collaboration avec des autorités suisses de protection des données (cantonales et fédérale).

1.38 Article 38

La commission reste formée de cinq membres, mais il est désormais précisé à l'al. 1 qu'elle doit contenir au moins deux juristes et un spécialiste en informatique. La commission est nommée par le Grand Conseil et fonctionne en qualité d'autorité judiciaire indépendante. Elle n'est pas un organe politique.

Le mandat de quatre ans est renouvelable. S'agissant d'une autorité collégiale, il ne semble pas nécessaire d'en limiter la durée. Il est simplement rappelé que les autres activités des membres de la commission doivent être compatibles avec leur fonction. Comme il s'agit d'une fonction à temps très partiel, il ne serait pas raisonnable d'exclure toute autre activité.

Son secrétariat n'est plus assuré par le préposé, les deux autorités étant indépendante. Il est proposé de rattacher administrativement la commission, en tant qu'organe judiciaire, au service parlementaire, dont elle pourra au besoin bénéficier de l'appui logistique. Cela ne remet pas en cause son indépendance et, au vu de son activité vraisemblablement assez réduite, voire irrégulière, la mise en place d'un secrétariat indépendant ne se justifie pas.

L'al. 2 prévoit que la commission se réunit au moins une fois par année et, pour le surplus, selon les affaires à traiter. Elle peut délibérer valablement en présence d'au moins trois de ses membres. Elle peut aussi consulter des experts externes si besoin (al. 3). Vu la fréquence à laquelle la commission se réunit, il n'est pas nécessaire que celle-ci dispose de locaux permanents.

Pour le surplus, le Grand Conseil règle l'organisation et le fonctionnement de la commission, ainsi que la rémunération de ses membres (al. 4). Il doit publier son règlement d'organisation.

1.39 Article 39

La commission fonctionnera en tant qu'autorité de décision de première instance, si un litige ne peut être réglé par le biais de la médiation. L'al. 1 prévoit qu'elle ne statue que sur les cas pour lesquels elle est saisie. Elle ne peut pas agir d'office, mais elle peut être saisie par le préposé, une autorité ou une personne concernée.

Les pouvoirs d'investigation de la commission sont identiques à ceux du préposé. Cela implique qu'elle peut exiger la production de pièces, demander des renseignements et se faire présenter des traitements. Les autorités concernées sont tenues de collaborer à l'établissement des faits. Elle peut en particulier, après prise de contact avec le responsable hiérarchique de l'autorité contrôlée, accéder en tout temps aux locaux où se trouvent des fichiers, se faire présenter ces derniers et les traitements de données, interroger le personnel, ainsi que demander des

renseignements et des pièces. Dans ce cadre, le secret de fonction ne peut pas lui être opposé.

L'al. 3 concerne les pouvoirs de la commission, notamment celui d'avertir l'autorité, d'ordonner la mise en conformité, la suspension ou la cessation de tout ou partie d'un traitement, l'effacement ou la destruction de tout ou partie des données, ainsi que de limiter voire interdire un traitement.

Finalement, l'al. 4 rappelle qu'elle doit publier son rapport d'activité conformément à l'art. 35 al. 4. La compétence de se prononcer sur des projets de lois a été supprimé vu qu'elle appartient désormais au préposé. Cela évite de trop solliciter la commission.

1.40 Article 52

Les dispositions de procédure et les voies de droit ont été intégralement revues en raison de la nouvelle définition des autorités de surveillance. La demande d'accès des anciens art. 48 à 50 est désormais traitée aux art. 12ss pour les documents officiels et 31ss pour les données à caractère personnel.

L'al. 1 oblige l'autorité qui n'entend pas donner suite à une demande d'en informer les intéressés et de leur indiquer qu'ils peuvent demander l'ouverture d'une procédure de médiation auprès du préposé conformément à l'art. 49. L'ancien délai pour demander l'ouverture d'une médiation n'est plus nécessaire puisque l'autorité n'est plus tenue de rendre une décision.

1.41 Article 53

Afin d'éviter un engorgement de la commission, il faut favoriser la médiation. Le préposé doit être assez libre dans sa manière de la conduire et il est renoncé à prévoir des règles de procédure contraignantes.

La médiation doit pouvoir être engagée dès qu'il y a une divergence à la suite d'une demande basée sur la LIPDA (al. 1bis). Tant l'autorité, le demandeur que le tiers intéressé doit pouvoir demander au préposé une médiation.

La procédure doit être simple, mais pour permettre un travail efficace du préposé, une requête écrite au moins sommairement motivée doit lui être adressée, accompagnée de toutes les pièces utiles.

Le préposé est libre de conduire la médiation comme il l'entend en fonction des circonstances. L'al. 2ter précise qu'il peut tenir une séance de médiation avec toutes les parties. Une telle séance n'est pas obligatoire, notamment si la situation est juridiquement claire et que le préposé peut déjà formuler une recommandation sur la base des informations en sa possession.

Dans le cas où une séance de médiation est convoquée, les parties peuvent assister à la médiation accompagnées de leur représentant. Il n'est pas nécessaire que le

préposé établisse un procès-verbal de la séance de médiation, sauf pour constater l'absence de l'une des parties. Si un accord est trouvé lors de la médiation, celui-ci est suffisant et le préposé n'a pas besoin de rendre un recommandation. Si aucun accord n'est trouvé, le préposé rend une recommandation qui doit intervenir dans les dix jours à compter de l'échec de la médiation. Ce délai peut être suspendu d'entente entre les parties. Lorsque l'une des parties ne comparaît pas, la médiation est réputée avoir échoué et des frais peuvent être mis à la charge de la partie qui ne s'est pas présentée.

1.42 Article 54a

L'al. 1 donne ainsi le droit de manière classique à l'autorité, au demandeur ou au tiers intéressé de saisir la commission lorsque la médiation n'a pas abouti. On considère que la médiation n'a pas abouti si aucun accord n'est trouvé et que l'autorité ne suit pas la recommandation du préposé, ou si le demandeur ou le tiers intéressé n'est pas satisfait de la recommandation du préposé (qu'elle soit ou non suivie par l'autorité) ou encore si l'accord trouvé n'est pas respecté.

Une saisine directe de la commission par une autorité ou une personne concernée, sans passer par la médiation, n'est pas prévue. Afin de s'assurer d'une application correcte de la LIPDA, le préposé peut en revanche aussi saisir spontanément la commission, indépendamment de l'avis des parties à la médiation, voire de l'absence de médiation. Cela permet par exemple de faire trancher un cas d'intérêt général, même si les parties n'y ont pas un intérêt direct, ou si une autorité ne respecte pas une recommandation du préposé.

La procédure devant la commission doit respecter les règles de procédure et le droit d'être entendu des parties doit être garanti, y compris celui du préposé (al. 2).

La consultation du préposé, voire la saisine par le préposé, doivent aussi faciliter le travail de la commission en lui permettant d'avoir un dossier à traiter aussi complet que possible. Il est primordial que la commission puisse bénéficier du maximum d'éléments possibles de la part du préposé, ce dernier pouvant se prévaloir de son expertise concrète du terrain et pour éviter qu'elle ne doive passer trop de temps à instruire les dossiers. Afin de respecter l'indépendance de la commission, elle reste cependant libre de mener tous les actes d'instructions qu'elle juge utiles.

1.43 Article 56

L'al. 1 est adapté, car désormais seules les décisions de la commission peuvent faire l'objet d'un recours au tribunal cantonal.

L'al. 2 est complété et assure le droit du préposé de recourir contre toute décision de la commission ou d'autorité appliquant la LIPDA, devant toutes les autorités

juridictionnelles cantonales et fédérales. Cela correspond à l'autonomie dont dispose le préposé.

L'al. 3 reprend la fin de l'ancien al. 1 et rappelle que la procédure est régie à titre supplétif par la loi sur la procédure et la juridiction administratives (LPJA).

L'al. 4 prévoit les normes de procédure liées à une demande de récusation formulée à l'encontre du préposé ou de l'un des membres de la commission. La Cour plénière du Tribunal cantonal est compétente pour se prononcer sur une telle demande de récusation. Si le Tribunal cantonal est partie à la procédure de récusation, le Grand Conseil est chargé d'examiner la requête de récusation.

1.44 Article 56a

Quelques droits particuliers doivent être garantis dans le cadre de la transposition de la Directive (UE) 2016/680. Il ne se justifie pas de changer pour autant l'intégralité du système prévu dans la LIPDA. Dès lors un nouveau titre 6a intitulé Disposition relative à la protection des données dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal est introduit, ainsi qu'un nouvel art. 56a.

Son champ d'application est limité aux données traitées dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal.

L'al. 1 let. a confère le droit à la personne concernée, et ce uniquement dans le cadre de l'application de l'acquis Schengen dans le domaine pénal, de faire appel au préposé pour procéder aux vérifications nécessaires lorsque certains de ses droits, sont retardés, limités, voire refusés.

Il est également ajouté un second droit particulier à l'al. 1 let. b. Il s'agit du droit pour la personne concernée de recourir directement au tribunal cantonal contre une décision d'autorité appliquant la LIPDA, pour autant que cela soit dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal. Ce droit de recourir direct est imposé par l'art. 54 de la Directive (UE) 2016/680.

1.45 Article T1-1

Le nouvel art. T1-1 concerne le traitement des données des personnes morales. Comme mentionné en commentaire de l'art. 3 al. 3, la protection des données des personnes morales n'est plus couverte par la présente loi, afin de s'aligner sur les choix faits aux niveaux fédéral et international. L'ensemble des actes législatifs valaisans doit tenir compte de ce changement. En effet, les bases légales qui autorisaient jusqu'à présent le traitement des données des personnes physiques et morales ne concernent plus que les personnes physiques. Ces différentes normes de droit cantonal doivent être adaptées pour justifier l'atteinte à la personnalité et aux droits fondamentaux des personnes morales. Une période transitoire de cinq ans est prévue dans cette disposition pour permettre ces modifications.

2. Modifications d’autres actes législatifs

La Directive (UE) 2016/680 a imposé une modification du Code pénal au niveau fédéral. En effet, afin de transposer les exigences de la Directive (UE) 2016/680, un certain nombre de dispositions de protection des données applicables aux échanges de données effectués dans le domaine de la coopération policière ont été introduite dans le Code pénal. A l’exception de certaines dispositions spécifiques, ces dispositions s’appliquent également aux autorités cantonales.

Les modifications d’autres actes n’appellent pas de commentaires particuliers.

Les autres modifications du droit en vigueur mentionnées dans le projet de loi sont reprises du précédent projet qui concernait uniquement l’adaptation de la LIPDA à la Directive (UE) 2016/680. L’exhaustivité des modifications du droit en vigueur n’a pas été vérifiée.

3. Conséquences financières et en ressources humaines

Le coût initial total, basé sur les standards de l’administration cantonale, peut être estimé entre 350’000 et 400'000 francs. Il comprend les postes du préposé et du secrétaire, le loyer des locaux ainsi que les frais divers.

Dois également être prévu un poste de délégué à la protection des données (juriste), personne indépendante qui serait soit engagée en interne à 100 % soit sur mandat. Les coûts annuels peuvent être estimés à 200'000 francs.

* * *