NOUVELLE LIPAD : les principaux changements à venir en matière de protection des données personnelles

FICHE INFO DU PPDT

PRÉAMBULE

L'art.13 al. 2 de la Constitution fédérale (RS 101; Cst.), ainsi que l'art. 21 al. 2 de la Constitution de la République et canton de Genève (RSGe A 2 00; Cst-GE) consacrent le droit de chacun d'être protégé contre l'emploi abusif des données qui le concernent. Faisant œuvre de pionnier, le législateur genevois s'est préoccupé d'assurer la protection de certaines données personnelles dès l'émergence des nouvelles technologies de l'information. La loi sur l'information du public et l'accès aux documents a été adoptée le 5 octobre 2001 et est entrée en vigueur le 1er mars 2002. En 2008, la loi a fait l'objet d'une révision importante: la protection des données personnelles a été ajoutée au volet transparence. La loi sur l'information du public et l'accès aux documents est ainsi devenue la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (LIPAD; RS/GE A 2 08). Depuis lors, de nombreuses évolutions ont eu lieu, tant d'un point de vue technologique, sociétal, que juridique, nécessitant une nouvelle adaptation de la LIPAD à ces développements, et notamment aux réformes du Conseil de l'Europe et de l'Union européenne en matière de protection des données personnelles, de même qu'à la révision du droit fédéral qui en découle. Les lois fédérales et cantonales en matière de protection des données mettent ainsi en œuvre la Convention 108+ du Conseil de l'Europe, qui a été ratifiée par la Suisse le 7 septembre 2023. Ces travaux sont indispensables pour que l'UE continue de reconnaître la Suisse comme un État tiers ayant un niveau de protection des données suffisant pour que la possibilité d'échanger des données avec elle soit préservée. La présente fiche info présente, en conséquence, les principaux changements apportés par la nLIPAD en matière de protection des données personnelles. Elle se veut un tour d'horizon non exhaustif qui devra être, de plus, complété par le RIPAD non encore finalisé.

DÉFINITIONS (art. 4 nLIPAD)

De manière générale, les définitions ont été adaptées en s'inspirant le plus possible de celles retenues par la nLPD, en vue de faciliter les futures interprétations par les autorités d'application. En plus des catégories de **données** sensibles déjà présentes, l'art. 4 nLIPAD ajoute les ***données génétiques*** et les ***données biométriques identifiant une personne physique de façon unique*** (litt. b ch. 5 et 6). Cette modification transpose les exigences de la Convention 108+ et de la directive (UE) 2016/68042, et est conforme à la nLPD. Les « données génétiques » sont toutes les données relatives aux caractéristiques héréditaires d'un individu ou acquises à un stade précoce du développement prénatal, résultant de l'analyse d'un échantillon biologique de cet individu : analyse des chromosomes, de l'ADN ou de l'ARN, ou de tout autre élément permettant d'obtenir des informations équivalentes. Quant aux « *données biométriques* », ce sont celles relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne, qui résultent d'un traitement technique spécifique et permettent ou confirment son identification unique. Il s'agit par exemple des empreintes digitales, des images faciales, de l'iris, ou encore de 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[1].

La lettre c mentionne une nouvelle notion, soit le ***profilage***, par lequel on entend "*toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects d'une personne, notamment pour analyser ou prédire des éléments concernant son rendement au travail, sa situation économique, sa santé, ses préférences personnelles, ses intérêts, sa fiabilité, son comportement, sa localisation ou ses déplacements*". Il est important de relever que le profil de la personnalité est le résultat d'un traitement et traduit ainsi quelque chose de statique. A l'inverse, le profilage se définit comme l'évaluation de certaines caractéristiques d'une personne sur la base de données personnelles traitées de manière automatisée afin notamment d'analyser ou de prédire son rendement au

[1] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 40.

travail, sa situation économique, sa localisation, sa santé, son comportement, ses préférences ou ses déplacements[2].

Une ***violation de la sécurité des données personnelles*** est instituée à la lettre j. Il s'agit de "*toute atteinte à la sécurité des données personnelles entraînant de manière accidentelle ou illicite leur perte, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces dernières*".

La lettre m, quant à elle, définit la ***décision individuelle automatisée*** comme "*toute décision prise exclusivement sur la base d'un traitement automatisé de données, y compris le profilage, et qui a des effets juridiques sur la personne concernée ou qui l'affecte de manière significative*" (litt. m). Ce type de décision ouvre de nouveaux droits pour la personne visée (art. 38B).

La définition de l'«***anonymisation***» a été ajoutée à la lettre k, pour une meilleure compréhension de cette notion. Le terme vise tout traitement de données personnelles consistant à supprimer définitivement toutes les données identifiantes ou tout moyen de retrouver les données originales. À noter que des données parfaitement anonymisées ne sont plus considérées comme des données personnelles, dans la mesure où elles ne permettent plus d'identifier une personne physique ou morale. L'« anonymisation » se distingue de la « pseudonymisation » en ce sens qu'elle est irréversible, contrairement à cette dernière[3].

Enfin, la notion de ***traitement*** est quelque peu étendue, dans le sens où l'utilisation, *l'extraction* et la *consultation* sont ajoutées aux moyens et procédés utilisés en relation avec une opération relative à des données personnelles (litt. d).

PRINCIPES FONDAMENTAUX

Selon l'art. 35 nLIPAD, tout traitement de données personnelles doit être ***licite*** et conforme aux principes de la ***bonne foi*** et de la ***proportionnalité***. De plus, les données personnelles ne peuvent être collectées que pour des ***finalités déterminées*** et ***reconnaissables*** pour la personne concernée et doivent être traitées ultérieurement de manière compatible avec ces finalités. La référence à des « finalités déterminées », à l'instar de la nLPD, indique qu'il n'est pas permis de traiter des données pour des finalités non définies, imprécises ou vagues[4]. Elles sont détruites, effacées ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement, dans la mesure où ces données ne doivent pas être conservées en vertu d'une autre loi. Sur décision de l'institution publique concernée, la destruction de données personnelles peut être différée durant deux ans au maximum à des fins d'évaluation de politiques publiques. De plus, quiconque traite des données personnelles doit s'assurer qu'elles sont ***exactes*** et prend toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données personnelles inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Cet art. 35 reprend les grands principes de traitement de données personnelles et est calqué sur la nLPD afin de faciliter les futures interprétations par les autorités d'application, et se rapproche, ce faisant, des textes européens[5].

De même, les institutions publiques ne peuvent traiter des données personnelles que si une ***base légale*** le prévoit ou si l'accomplissement de leurs tâches légales le rend nécessaire (art. 36 al. 1er nLIPAD). À ce propos, les traitements de données personnelles sensibles et les activités de profilage ne peuvent avoir lieu que si une loi au sens formel le prévoit expressément ou que le traitement est indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel. Enfin, ***en dérogation*** aux alinéas 1 et 2, les institutions publiques peuvent traiter des données personnelles nécessaires à l'accomplissement de leurs tâches légales, y compris des données personnelles sensibles, et procéder à du profilage, si l'une des conditions énumérées aux lettres a à c de l'art. 36 al. 3 nLIPAD est donnée, soit notamment en cas de ***consentement au traitement*** d'espèce de la personne concernée. Le consentement n'est valable que si la personne concernée exprime librement sa volonté concernant un ou plusieurs traitements déterminés et après avoir dûment été informée (al. 4)[6]. Le consentement doit être ***exprès pour le traitement de données personnelles sensibles et le profilage*** (al. 4 in fine) et ***peut être révoqué en tout temps*** (al. 5). Pour que le consentement soit valable, il faut toujours que le traitement, en particulier son ampleur et son but, soit suffisamment défini. Le consentement peut porter sur plusieurs traitements identiques ou différents. Il est également possible que le but du traitement nécessite

[2] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 41.
[3] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 42.
[4] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 47.
[5] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 52.
[6] Quant au devoir d'informer lors de la collecte de données personnelles, cf. art. 38 nLIPAD.

plusieurs traitements[7]. À noter que le consentement ***doit rester une exception*** en tant que fait justificatif extra-légal au traitement de données personnelles et ne saurait justifier des traitements systématiques de données personnelles[8].

MESURES VISANT A GARANTIR LA PROTECTION DES DONNEES

La nLIPAD renforce les obligations des responsables de traitement afin de garantir la protection des données et ce, par diverses mesures.

Protection des données personnelles dès la conception et par défaut (art. 37 nLIPAD)

Selon l'art. 37 nLIPAD, le responsable du traitement doit mettre en place des "***mesures techniques et organisationnelles***" dès les premières étapes de la conception des opérations de traitement, afin que celui-ci respecte le plus tôt possible les prescriptions de protection des données personnelles. Il s'agit de respecter, en particulier, les principes fondamentaux prescrits à l'art. 35 nLIPAD (*licéité, bonne foi et proportionnalité, finalité et reconnaissabilité, conservation, destruction, effacement et anonymisation, exactitude*). Ces mesures doivent être ***appropriées*** (par exemple au regard de l'état de la technique ou du type de traitement et son étendue). Par le biais de ***préréglages appropriés***, le responsable garantit ainsi que le traitement est limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement. De même, ces mesures se doivent d'être *appropriées face au risque* que le traitement de données présente pour la personnalité ou les droits fondamentaux des personnes concernées. Cette disposition est calquée sur l'article 7 nLPD, afin de faciliter les futures interprétations par les autorités d'application, et met en œuvre, à l'instar de ce dernier, les exigences de la Convention 108+ et de la directive (UE) 2016/680[9]. La protection des données *par défaut* ne doit pas être confondue avec la protection des données *dès la conception*, qui exige de traiter le moins de données possibles par des préréglages appropriés. Les deux principes n'en restent pas moins étroitement liés, dans la mesure où de telles fonctionnalités doivent être intégrées dès la conception[10].

Sécurité des données personnelles et violation de la sécurité des données personnelles – devoirs d'annonce (art. 37A et 37C nLIPAD)

Les violations de données personnelles sont de plus en plus fréquentes. Elles constituent un non-respect, involontaire ou de source malveillante, du principe de la sécurité des données (consacré par l'art. 37A LIPAD). Ces violations peuvent intervenir auprès de l'institution publique elle-même ou auprès d'un sous-traitant. La LIPAD, dans sa version du 3 mai 2024, a introduit des **obligations pour le responsable de traitement et pour le sous-traitant** en cas de violation de la sécurité des données personnelles. Toute institution publique qui traite de données personnelles doit en garantir la sécurité. L'art. 37A LIPAD prévoit à cet égard que : *[1] Les institutions publiques doivent assurer, **par des mesures organisationnelles et techniques appropriées**, une sécurité adéquate des données personnelles par rapport au risque encouru. [2] Les mesures doivent **permettre d'éviter la violation** de la sécurité des données personnelles. [3] Le Conseil d'État détermine, par voie réglementaire, les exigences minimales en matière de sécurité des données personnelles. [4] Les institutions publiques sont tenues de **contrôler périodiquement le respect des mesures de sécurité** mises en place au sens du présent article*.

À titre d'**exemple** de violation de données personnelles, on peut mentionner l'envoi de données personnelles à un mauvais destinataire (ex : mail envoyé par erreur), la perte d'un ordinateur sur lequel les données ne sont pas chiffrées, une cyberattaque, l'accès aux données par des autorités étrangères, etc. Dans tous les cas de violations de données, le conseiller ou la conseillère LIPAD de l'institution publique concernée doit être informé/e de la violation des données et associé/e aux démarches entreprises. Il en va de même si la violation des données est intervenue auprès d'un sous-traitant.

Quelle que soit la nature de la violation, l'institution publique confrontée à un tel incident doit documenter précisément les éléments relatifs aux points susmentionnés, afin de pouvoir y remédier de manière optimale. En effet, l'envoi d'un courriel au mauvais destinataire ne nécessite pas le même type de mesures qu'être victime d'une intrusion malveillante dans ses systèmes informatiques. Une fois ce premier bilan établi, l'institution publique pourra déterminer quelles mesures techniques ou organisationnelles devront être prises pour mettre fin à la violation ou en minimiser les effets,

[7] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 52.
[8] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 52.
[9] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 57.
[10] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 57 s.

comme l'exige l'art. 37C al. 1 LIPAD. De plus, si la violation est constitutive d'une infraction pénale (art. 143 – soustraction de données – et 143bis CP – accès indu à un système informatique –), une plainte peut être déposée.

Les mesures préconisées ci-dessus doivent être mises en place également en cas de **cyberattaque**. En cas *d'intrusion dans ses systèmes informatiques*, il appartient, en plus, à l'institution publique, de reprendre le contrôle sur les données, dans les meilleurs délais, en prenant contact avec son service informatique. Si les connaissances requises font défaut à l'interne, il sied de faire appel à une entreprise de sécurité informatique. L'on peut se référer au site internet du centre national pour la cybersécurité (NCSC) qui propose plusieurs aide-mémoires, selon différents cas de figure[11]. Une telle attaque peut d'ailleurs lui être annoncée[12].

Selon l'art. 37C al. 3 LIPAD, le responsable de traitement doit **annoncer** au Préposé cantonal les cas de violation de la sécurité des données personnelles entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, dans les meilleurs délais. Une ***notification* au PPDT** est donc prévue lorsque le cas de violation entraîne « *un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée* ». Une évaluation devra intervenir au cas par cas. La question à se poser est la suivante : quelle est la probabilité (faible, moyenne, élevée) que la violation ait une conséquence négative déterminée? Dans cet examen, la nature et le type de données, le type de violation, le nombre de personnes concernées notamment doivent être prise en considération[13]. Le **but** d'une telle annonce est que le Préposé cantonal puisse suivre la situation et prodiguer des conseils sur les mesures à prendre et sur l'éventuelle nécessité d'informer les *personnes concernées*.

Analyse d'impact (AIPD) (art. 37B nLIPAD)

Depuis le 1er septembre 2023, au niveau fédéral, une nouvelle obligation a vu le jour, qui prescrit que tout traitement de données pouvant mener à un risque élevé doit faire l'objet d'une analyse d'impact relative à la protection des données personnelles (AIPD) (art. 22 et 23 de la loi sur la protection des données révisée (LPD[14]). Il s'agit d'un **instrument destiné à identifier et à évaluer les risques que certains traitements de données personnelles pourraient entraîner pour la personne concernée**. Le cas échéant, l'AIPD doit servir à définir des mesures pour faire face à ces risques. Ainsi, le responsable du traitement peut anticiper d'éventuels problèmes juridiques liés à la protection des données et ainsi éviter les coûts qui pourraient en résulter[15].

Dans cette lignée, à Genève, la LIPAD a été modifiée afin de l'adapter aux développements technologiques et juridiques intervenus depuis son entrée en vigueur, le 1er mars 2002, tels que rappelés en préambule de cette fiche info. Une nouvelle base légale – qui s'inspire en grande partie de la nouvelle LPD[16] – a, dès lors, été adoptée. Elle impose une analyse d'impact lorsqu'un traitement de données personnelles est susceptible d'entrainer un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 37B nLIPAD). L'AIPD est un instrument de travail du droit moderne de la protection des données, qui vise à préserver les droits des personnes concernées en identifiant à un stade préalable les risques élevés associés à un projet, caractérisés par leur probabilité de survenance et la gravité de leurs conséquences (*risques élevés*)[17]. Ainsi, la simple possibilité d'un risque ne suffit pas à entrainer l'obligation de mener une analyse d'impact. La loi impose, en effet, que ce "***risque***" soit "***élevé***". Pour apprécier ce qui, dans un cas d'espèce, représente un tel risque, il faut, en premier lieu, examiner si le traitement concerné tombe sous le coup des exemples dressés par l'art. 37B al. 2 let. a à c nLIPAD. Si tel est le cas, alors l'analyse d'impact est obligatoire[18].

L'AIPD peut intervenir dans **deux situations** au sens de l'art. 37B nLIPAD soit : à l'occasion de l'établissement d'un projet d'acte législatif (al. 4) ou en dehors d'un tel projet (al. 5). Dans le premier cas, l'AIPD doit être jointe au projet pour avis du ou de la Préposé/e cantonal/e (au sens de l'art. 56A al. 2 let. e nLIPAD) ; dans le **second cas, l'analyse d'impact est soumise au Préposé ou à la Préposée cantonal/e pour avis avant** le début du traitement. Il faut retenir

[11] Cf. https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-behoerden/vorfall-was-nun.html.
[12] Cf. https://www.report.ncsc.admin.ch/fr/.
[13] MÉTILLE Sylvain / MEYER Pauline, Annonce des violations de la sécurité des données : une nouvelle obligation de la nLPD, RSDA 1/2021, p. 26.
[14] RS 235.1.
[15] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 37.
[16] De ce fait, il est donc souvent possible de se référer à ce qui a été dit / est dit en relation avec la LPD.
[17] https://www.edoeb.admin.ch/dam/edoeb/fr/Dokumente/datenschutz/merkblatt_dsfa.pdf.download.pdf/Merkblatt_DSFA_FR.pdf, ch. 2 p. 4.
[18] Si tel n'est pas le cas et en relation avec l'art. 22 al. 2 LPD sur le même sujet mais **au niveau fédéral**, il est tout de même opportun d'examiner alors les listes noires dressées par les autorités de contrôle européennes, non contraignantes en Suisse mais qui fournissent des lignes directrices importantes (CR LPD – GILLIÉRON, N28, 33- 38 et les réf. citées). **Au niveau cantonal**, rien encore n'a été édicté en la matière mais il s'agira d'y rester attentif.

cependant que – toutes conditions remplies au demeurant –, il s'agit d'une obligation pour laquelle le droit genevois ne prévoit pas d'exception. En la matière, la compétence du Préposé cantonal / de la Préposée est renforcée dans les sens précités[19].

AUTRES DISPOSITIONS SENSIBLEMENT MODIFIÉES

Traitement à des fins générales ne se rapportant pas à des personnes (art. 41 nLIPAD)

Cette disposition vise **deux situations** : premièrement, celle où une institution publique traite les données qu'elle détient à des fins ne se rapportant pas à des personnes et deuxièmement, celle où elle communique les données à des organes de la Confédération ou des cantons, ou encore à des personnes privées, *à des fins de recherche, de planification ou de statistique*. L'alinéa 1 énonce à quelles conditions cumulatives une institution publique peut invoquer le *privilège de la recherche*[20]. Il est **important de relever que** dans ces cas, les principes de *finalité* et *reconnaissabilité* ne s'appliquent pas, de même que l'art. 36 al. 2 et 39 nLIPAd (art. 41 al. 2 nLIPAD).

Le **changement principal** apporté par cet article **est** qu'il n'y a plus d'annonce à faire au Préposé cantonal en cas de traitement de données personnelles "ordinaires", ni d'autorisation du Conseil d'État avec préavis au Préposé cantonal en cas de traitement de données personnelles sensibles. De plus, il est possible de **réutiliser** des données **pour une autre finalité (mentionnée à l'art. 41 nLIPAD)** que celle pour laquelle elles ont été collectées.

Sous-traitance (art. 36C nLIPAD)

Cet article reprend, pour l'essentiel, la teneur de l'article 13A aRIPAD. Il précise de plus, à son alinéa 1er litt. a, que seuls les traitements que le responsable du traitement est en droit de réaliser peuvent être sous-traités. Les alinéas 1 et 2 posent le cadre légal général de la sous-traitance.

Registre des activités de traitement (art. 43 nLIPAD)

L' aLIPAD contenait déjà, à son article 43, le catalogue des fichiers (CATFICH). Du fait de la **disparition** de la notion de **fichier** et de son **remplacement** par la notion de **traitement**, ce catalogue des fichiers est désormais intitulé *registre des activités de traitement* des institutions publiques[21]. Selon la nouvelle disposition, la Préposée cantonale ou le Préposé cantonal *dresse et tient à jour un registre public des activités de traitement des institutions publiques*, qu'elle/il *rend facilement accessible* (al. 1er). Les institutions publiques doivent déclarer leurs activités de traitement au Préposé ou à la Préposée cantonal/e, en fournissant au moins les indications mentionnées aux lettres a à e de l'alinéa 2. Dans ce cadre, les informations publiques figurent au registre des activités de traitement tenu par le Préposé cantonal. La Préposée cantonale ou le Préposé cantonal peut demander d'autres indications, précisées à l'al. 3. Ces informations ne figurent pas dans le registre, mais doivent être disponibles sur demande du Préposé cantonal.

Les **informations de l'ancien catalogue des fichiers seront automatiquement transférées** dans le registre des traitements. Il appartiendra aux conseillères et conseillers LIPAD de les passer en revue afin de s'assurer que toutes les nouvelles informations nécessaires y figurent.

DROITS DES CITOYEN-NE-S EN MATIÈRE DE PROTECTION DES DONNÉES (art. 38B et 44 ss nLIPAD)

Comme exposé ci-avant, l'art. 4 litt. m nLIPAD définit la ***décision individuelle automatisée*** comme une décision prise exclusivement sur la base d'un traitement automatisé de données, y compris le profilage, et qui a des effets juridiques sur la personne concernée ou qui l'affecte de manière significative. L'introduction de la notion de décision individuelle automatisée est nécessaire, car ces décisions sont de plus en plus fréquentes en raison du développement technologique. Une décision individuelle automatisée implique en tout cas qu'il n'y ait eu aucune décision prise par une personne physique sur la base de sa propre évaluation de la situation. Ainsi, **il y a décision individuelle automatisée**

[19] Au surplus, cf. la fiche info du PPDT sur l'analyse d'impact à venir.
[20] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 72.
[21] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 75.

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. Seules les décisions qui sont **entièrement prises par une machine et** qui supposent un **pouvoir d'appréciation** sont concernées, c'est-à-dire celles qui requièrent une évaluation ou une interprétation[22]. Une telle décision **a des effets juridiques sur la personne concernée** ou **l'affecte de manière significative**. Ce type de **décision** ouvre de **nouveaux droits** pour la personne visée.

En effet, l'art. 38B nLIPAD énonce que *[l]e responsable du traitement **informe** la personne concernée de toute décision qui est prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour elle ou l'affecte de manière significative (al. 1er)*. À ce propos, il n'est 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**, c'est-à-dire lorsqu'elle est **durablement entravée** sur le plan économique ou personnel. Une simple nuisance ne suffit pas[23]. Selon l'alinéa 2, sur demande de la personne faisant l'objet d'une telle décision, "*le responsable du traitement lui **communique** la logique et les critères à la base de celle-ci*", étant entendu que "*[c]ette demande ne suspend pas le délai visé à l'alinéa 3*". Cet alinéa 3 précise que *[t]oute personne faisant l'objet d'une décision individuelle automatisée **peut former une réclamation**, dans les 30 jours à compter de sa notification, auprès de son auteure ou auteur. De plus, il faut relever que, [l]a décision sur réclamation ne peut pas être rendue de manière automatisée (al. 5)* ; ceci, afin de garantir qu'une personne physique examine la réclamation d'espèce[24]. Enfin, *[l]es dispositions de la législation spéciale qui prévoient déjà une procédure de réclamation* sont réservées par l'alinéa 6.

Les art. 44 ss nLIPAD **reprennent** la notion du ***droit d'accès*** déjà connue dans la LIPAD actuelle, **en l'adaptant** à l'évolution du droit supérieur, ainsi que les **principes** de ce droit. La nLPD, la Convention 108+ et la directive (UE) 2016/680 notamment, contiennent des dispositions similaires. Le droit d'accès complète l'obligation d'informer du responsable du traitement. Il est la clé qui permet à la personne concernée de faire valoir les droits que lui octroie la loi[25].

L'alinéa 1er de l'art 44 nLIPAD, quant à lui, dispose que toute ***personne physique*** ou ***morale de droit privé*** peut demander ***par écrit au responsable du traitement, en s'adressant à la conseillère ou au conseiller à la protection des données et à la transparence*** (au sens de l'art. 50) de ce dernier, si des données personnelles la concernant sont traitées. Le but de la loi n'est pas de conférer aux institutions de droit public qui lui sont soumises des droits spécifiques à cet égard. Il est dès lors précisé que **ce catalogue de droits ne concerne que les personnes de droit privé**[26]. Le droit d'accès ne dépend, en outre, d'***aucun intérêt particulier***. Cela signifie qu'il n'y a aucune restriction liée à la nationalité, au domicile ou à l'âge, voire à la personnalité du demandeur ou à l'usage qu'il compte faire de ses données. Le demandeur ne doit nullement motiver sa demande. **Par rapport au droit en vigueur**, la ***justification de l'identité*** est transférée dans l'article 45 al. 1er, relatif aux **modalités**. Il est, par ailleurs et désormais, fait référence au responsable du traitement, par le biais de sa conseillère ou son conseiller LIPAD, et **non plus au responsable LIPAD**[27].

Cette disposition met en lumière non seulement le lien étroit qui existe entre le droit d'accès et le devoir d'informer, mais aussi le **but fondamental du droit d'accès**, soit de permettre à la personne concernée[28] de faire valoir ses droits en matière de protection des données. Ainsi, le droit d'accès **vise uniquement** à aider une personne concernée à faire valoir ses droits en matière de protection des données (au moins ses droits pouvant faire l'objet d'une action en justice) et à garantir la transparence du traitement des données (p. ex. pour permettre à une personne de savoir quelles données une institution publique détient à son sujet). Les **lettres a à f** donnent une **énumération non exhaustive** des informations qui doivent être communiquées dans tous les cas à la personne concernée. Lorsqu'elle traite des quantités

[22] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 70.
[23] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 70.
[24] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 71.
[25] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 76.
[26] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 76.
[27] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 76s.
[28] À noter que le droit d'accès est un **droit subjectif inhérent à la personne**, que même une personne qui n'a pas l'exercice des droits civils mais qui est capable de discernement peut faire valoir seule, sans avoir à requérir le consentement de son représentant légal. Le fait que ce droit est inhérent à la personne a pour conséquence que nul ne peut y renoncer par avance (Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 78.)

importantes de données sur celle-là, la personne tenue de fournir les renseignements doit pouvoir lui demander depréciser sur quelles données ou quelles opérations de traitement porte sa requête[29]. Une **réponse écrite**[30] et **gratuite**

doit être fournie **dans les 30 jours** (art. 45 al. 2, 3 et 4 nLIPAD), sous réserve d'exceptions prévues par le Conseil d'État, notamment en cas de travail disproportionné (art. 45 al. 3 et 4 nLIPAD). Un **accès partiel** est toujours préférable à un refus[31].

À noter que le **débiteur du droit d'accès est** toujours le responsable du traitement **même si** celui-ci confie le traitement à un **sous-traitant**[32] (art. 44 al. 3 nLIPAD).

Quant à **ce que peut obtenir le/la citoyen/ne**, l'art. 47 al. 2 lit. a, d et e dans leur nouvelle teneur prescrit le droit d'obtenir que l'institution publique ***efface*** ou ***détruise*** les données non nécessaires, qu'elle ***s'abstienne de communiquer*** celles qui ne répondent pas aux exigences de qualité visées à l'art. 35 et ***publie*** sa décision suite à la requête ou la ***communique*** aux institutions ou tiers ayant reçu de sa part des données qui ne répondent pas auxdites exigences. De plus, le responsable du traitement doit traiter la requête avec ***célérité*** (art. 49 al. 2 nLIPAD). Enfin, l'institution publique concernée statue par voie de ***décision dans les 30 jours***[33] et la ***notifie*** à la ***Préposée cantonale /au Préposé cantonal*** (art. 49 al. 3 nLIPAD) qui dispose d'un ***droit de recours*** (art. 62 aLIPAD/nLIPAD). Il faut relever qu'à l'instar de ce qui découle déjà de l'actuelle LIPAD, le droit d'obtenir des institutions les actions sollicitées **n'existe que « *sauf disposition légale contraire* »**, afin de réserver notamment aussi bien les règles particulières de la loi sur les archives publiques, du 1er décembre 2000 (LArch; rs/GE B 2 15), relatives à la destruction des dossiers, que celles de la loi sur la santé, du 7 avril 2006 (LS; rs/GE K 1 03), en particulier l'article 57 de cette dernière qui traite de la conservation du dossier du patient[34]. **Contrairement à ce qui était le cas sous l'aLIPAD** (art. 49 al. 4 et 5), l'institution qui n'entend pas donner une suite favorable à la demande n'a **plus à saisir le PPDT** pour qu'il établisse une recommandation écrite sur la suite à donner à la requête.

RÔLE DES CONSEILLÈRES ET CONSEILLERS LIPAD (art. 50s nLIPAD)

Le conseiller ou la conseillère LIPAD désigné/e par chaque institution publique joue un **rôle clé** dans la mise en œuvre de la loi. Il/elle est le **relais** du Préposé ou de la Préposée cantonal/e (art. 51 al. 1er nLIPAD), comme c'était d'ailleurs le cas jusqu'à présent. Il faut relever que plusieurs institutions publiques peuvent en désigner un ou une ensemble (art. 50 al. 2 nLIPAD).

La LIPAD actuelle prévoit déjà que des responsables ayant une ***formation appropriée*** et les ***compétences utiles*** doivent être désignés au sein des institutions, pour y garantir une correcte application de la LIPAD. Les travaux préparatoires de la LIPAD actuelle précisaient à cet égard que les responsables des institutions sont la cheville ouvrière du nouveau dispositif. Il s'agit donc d'apporter un soin tout particulier dans leur désignation afin de faciliter au mieux l'efficacité de leur action. Il ne s'agit **pas** cependant de **définir de manière trop rigide** les compétences et le niveau de formation attendus des futures et futurs conseillères/ers LIPAD, tant les institutions ont des moyens en personnel et en budget qui peuvent se révéler différents[35]. La terminologie est toutefois adaptée au droit fédéral, les responsables LIPAD étant désormais dénommés « conseillères et conseillers à la protection des données et à la transparence ». Cette fonction est également prévue dans la directive (UE) 2016/680[36].

En matière de protection des données, seules **deux nouvelles tâches** sont expressément mentionnées dans la nLIPAD : concourir à l'établissement des analyses d'impact (art. 51 al. 3 lit. b) **et** annoncer au Préposé ou à la Préposée cantonal/e les violations de la sécurité des données personnelles entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée qui leur ont été communiquées par le responsable du traitement (art. 51 al. 3 lit. d).

---

[29] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 77.
[30] En accord cependant avec le responsable du traitement, la personne physique ou morale de droit privé concernée peut consulter ses données sur place (art. 45 al. 2 2ème phrase nLIPAD).
[31] Pour les **restrictions d'accès** aux données personnelles, cf. l'art. 46 aLIPAD/nLIPAD.
[32] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 78.
[33] Il s'agit toujours d'un **délai d'ordre** (Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 80).
[34] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 79.
[35] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 80s.
[36] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 81.

POUVOIRS DE CONTRÔLE ET MESURES ADMINISTRATIVES DU PPDT (art. 56A ss nLIPAD)

L'art. 56A nLIPAD reprend la teneur de l'article 56, alinéa 3, de l'aLIPAD. L'alinéa 1er introduit, de manière générale, la **mission** de la Préposée cantonale ou du Préposé cantonal en matière de protection des données personnelles.

L'art. 56B nLIPAD prévoit de **renforcer les moyens d'intervention** de la Préposée cantonale ou du Préposé cantonal, conformément aux nouveaux standards des lois de protection des données, que ce soit la nLPD, la Convention 108+, la directive (UE) 2016/680. Elle/il pourra, par exemple, effectuer un contrôle d'office ou sur dénonciation, auprès d'une institution publique ou d'un sous-traitant, afin de vérifier qu'ils respectent les dispositions de protection des données personnelles, en décidant librement, au demeurant, des contrôles qu'elle/il veut effectuer ou de la suite à donner à une dénonciation (art. 56B al. 1er nLIPAD). Les alinéas 3 et 4 traitent du ***devoir de collaboration*** des institutions et des sous-traitants et de la problématique du ***secret de fonction***, et ***autres secrets*** institués par la loi, qui y est liée. La Préposée cantonale ou le Préposé cantonal ***peut*** ainsi, notamment, ***demander*** des renseignements, exiger la production de documents, procéder à des inspections et se faire présenter des traitements de donner. Il peut également recourir, au besoin, à des expertes et experts dans les domaines techniques (al. 2). Le secret de fonction ne peut pas lui être opposé dans ce cadre. Les autres secrets institués par la loi sont toutefois réservés (al. 3).

L'art. 56C permet à la Préposée cantonale ou au Préposé cantonal de prendre des ***mesures administratives***, mais ne l'y oblige pas. Une **grande marge de manœuvre** lui est ainsi laissée. Cette disposition contient deux catégories de mesures. La première catégorie (al. 1er et 2) prévoit un **catalogue de mesures** contre des traitements de données contraires à des dispositions de protection des données. Le principe de base de cette réglementation est le **respect du principe de proportionnalité**. Ainsi, au lieu d'ordonner la cessation du traitement, la Préposée cantonale ou le Préposé cantonal peut ordonner sa modification et limiter la mesure à la partie du traitement problématique. La **seconde catégorie** (al. 3) concerne des cas de non-observation de prescriptions d'ordre ou de devoirs à l'égard de la personne concernée. Parmi les **compétences décisionnelles** qui sont attribuées à la Préposée cantonale ou au Préposé cantonal, celle-ci ou celui-ci peut, par exemple, ordonner à l'institution publique de procéder à une analyse d'impact au sens de l'art. 37B nLIPAD (lit. g)[37]. À relever que ***si une institution publique ne donne pas suite à l'ordre*** du ou de la **Préposé/e** cantonal/e, au sens de l'alinéa 3, il ou elle ***peut saisir les instances compétentes*** (art. 50 al. 3 et 4 nLIPAD) qui prescriront par ***substitution*** les mesures nécessaires (al.4). Par contre, la Préposée cantonale ou le Préposé cantonal ne **disposera pas du pouvoir de prononcer des sanctions administratives** à l'encontre des institutions[38].

Enfin, l'art. 56C prévoit que la **procédure** est régie par la loi sur la procédure administrative, du 12 septembre 1985 (al. 1er)[39] et que **l'institution publique visée** par une décision du Préposé ou de la Préposée cantonal/e a qualité pour recourir contre celle-ci (al. 2). Seule celle-ci peut recourir contre les mesures prononcées contre elle par la Préposée cantonale ou le Préposé cantonal[40]. Ainsi, la **personne concernée n'a pas qualité de partie** à la procédure, même si la Préposée cantonale ou le Préposé cantonal a ouvert l'enquête sur dénonciation de celle-ci. Si elle entend faire valoir des prétentions d'une institution publique responsable du traitement, elle doit procéder selon l'article 49 (ou 44 ss nLIPAD), en recourant, le cas échéant, contre la décision de l'institution publique responsable du traitement auprès de la chambre administrative de la Cour de justice[41].

PPDT – 19.12.24

[41] Grand Conseil, Projet de loi modifiant la LIPAD, 5 juillet 2023, PL 13347, p. 87.