Projet de loi sur la simplification administrative et les référentiels cantonaux des données de base des personnes (mise en œuvre du principe once only)

Avis du 23 juin 2025

Mots clés: données personnelles, données de base, communication de données, once only, simplification administrative, coffre-fort numérique, consentement

Contexte: En date du 30 mai 2025, le responsable LIPAD du Département des finances, ressources humaines et affaires extérieures (DF) a sollicité l'avis du Préposé cantonal à la protection des données et à la transparence (Préposé cantonal), dans le cadre d'un projet de loi sur la simplification administrative et les référentiels cantonaux des données de base des personnes (mise en œuvre du principe once only). Le projet de loi (PL) introduit et met en œuvre l'objectif de simplification administrative au sein des institutions publiques en faveur des usagères, des usagers et des entreprises, en dotant ces institutions des outils et référentiels de données personnelles nécessaires à l'allègement des démarches administratives. Il prévoit deux volets distincts : les référentiels cantonaux des données de base des personnes (personnes physiques, personnes morales et entreprises), et les principes et règles selon lesquels les institutions publiques ne sollicitent qu'une seule fois les données personnelles et documents nécessaires à la délivrance des prestations.

Bases juridiques: art. 56 al. 2 litt. e et art. 56 al. 3 litt. e LIPAD; art. 23 al. 8 RIPAD

1. Caractéristiques de la demande

Par courrier électronique du 30 mai 2025, le responsable LIPAD du Département des finances, ressources humaines et affaires extérieures (DF) a sollicité l'avis du Préposé cantonal à la protection des données et à la transparence (Préposé cantonal), dans le cadre d'un projet de loi sur la simplification administrative et les référentiels cantonaux des données de base des personnes (mise en œuvre du principe once only).

Selon l'exposé des motifs, "*Le présent projet de loi ambitionne, à l'aide d'outils concrets et cohérents, de simplifier les démarches administratives des usagères, des usagers et des entreprises avec l'administration de l'Etat de Genève, de même qu'avec possiblement - compte tenu de leur autonomie - les communes et les principaux établissements autonomes de droit public du canton. A cette fin, le texte dote ces institutions publiques des outils de gestion et des règles nécessaires à la mise en œuvre de l'objectif de simplification administrative.*

Il comporte, selon le principe once only, les règles visant à réutiliser autant que possible les données de base des personnes, ainsi que les autres données et documents requis à la délivrance des prestations, qui sont éventuellement déjà en possession des institutions publiques, au sujet desquels les usagères et usagers conservent toutefois l'entière maîtrise.

L'ensemble du dispositif doit contribuer de manière significative à simplifier les interactions des usagères et usagers avec les administrations, avec à la clé des économies de moyens et de temps de part et d'autre.

De surcroît, le projet améliore l'efficacité et l'efficience de la délivrance des prestations par les collectivités publiques précitées, en dotant celles-ci de référentiels de données de base des personnes, qui soient autant que possible exactes et actuelles, cela conformément aux objectifs poursuivis par les législations fédérales et cantonales, ainsi que conventionnelles, en matière de protection des données personnelles.

Le présent projet de loi concrétise notamment l'objectif 4.3 du Conseil d'Etat décrit dans son programme de législature 2023-2028, visant à renforcer la cyberadministration pour mieux servir la population et les entreprises.

Saisissant les opportunités qu'offre le numérique pour rendre les prestations de l'administration plus accessibles à la population, le Conseil d'Etat entend simplifier les démarches des usagères et usagers, avec l'ambition notable de ne collecter qu'une seule fois l'information selon le principe du once only et de la partager au sein de l'administration, tout en respectant l'intégrité des personnes. Ce partage ne peut se faire sans l'accord éclairé de la personne. Par ailleurs, il encourage le développement de l'offre en ligne et évite la fracture numérique en accompagnant la population dans son utilisation" (p. 19).

Globalement, le projet a 2 objectifs:

- Simplifier les démarches administratives pour les usagers et usagères (principe du once only – permettre à l'usager de déposer une seule fois un document nécessaire à la délivrance de plusieurs prestations)
- Doter les institutions publiques et certaines entités de droit privé chargées d'exécuter des tâches de droit public de données de base (exhaustivement listées dans le projet) fiables, univoques, actuelles et exactes.

Il repose notamment sur la Déclaration de Tallinn sur l'administration en ligne signée le 6 octobre 2017 par le Conseil fédéral, la loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes, du 23 juin 2006 (LHR; RS 431.02), ainsi que sur l'art. 9 de la Constitution de la République et canton de Genève, du 14 octobre 2012.

Les Préposés ont été sollicités pour accompagner le projet à diverses étapes:

- Une première présentation du projet est intervenue le 12 septembre 2024.
- Une nouvelle version du projet a été communiquée aux Préposés le 14 octobre 2024, prenant en compte diverses remarques formulées lors de la séance du 12 septembre 2024, en lien notamment avec la journalisation des consultations (art. 17), les références à la mission légale de l'institution (art. 11), ou encore la conservation des informations dans les applications métier (art. 12).
- Par courriel du 28 octobre 2024, les Préposés ont relevé quelques éléments qui méritaient d'être précisés dans le projet:
    - S'agissant des référentiels de données de base, ils suggéraient de clarifier les appariements (quelles sont les bases de données sources qui vont nourrir les référentiels?), les responsabilités en cas de contradictions entre les données contenues dans les bases "métier" et celles dans les référentiels. Ils suggéraient que la gestion des accès soit abordée dans le projet de loi (qui les octroie et à quelles conditions?) ou à tout le moins en prévoir le principe par délégation réglementaire tout en en précisant les principes principaux au niveau de la loi. Finalement, se posait la question du cycle de vie des données. La finalité des référentiels étant l'identification et la localisation des personnes concernées, le responsable de traitement devrait être l'institution publique qui a cette mission.
    - S'agissant du coffre-fort numérique et de l'échange de données, il reposait sur le consentement du citoyen, de sorte que la question de la validité

dudit consentement se posait: il importait ad minima que figurent la finalité pour laquelle les données / documents peuvent être utilisés, l'étendue du traitement, et que les services qui accèdent aux données soient connus de la personne concernée, principes qui pourraient être précisés dans le projet. Le principe de la proportionnalité devait être respecté par des accès différenciés. Ici aussi, les règles concernant la gestion des accès devraient être abordées dans le projet de loi, du moins quant à leur principe (droits et conditions d'accès). De plus, il est de la responsabilité des institutions publiques de s'assurer qu'elles n'ont pas accès à des données dont elles n'ont pas besoin dans le cadre de leurs tâches légales; le projet de loi devrait mieux encadrer cela.

- De manière générale, les Préposés avaient souligné que le danger perçu, à la lecture du projet de loi, libellé de manière très large de sorte qu'il pourrait couvrir l'intégralité des activités de l'administration, revenait à ce qu'il y ait une sorte de gigantesque base unique avec des informations se rapportant à toutes les sphères de la vie du citoyen. Cela serait, malgré son consentement, potentiellement extrêmement intrusif en termes de protection de sa sphère privée. L'enjeu en matière de sécurité des données avait été souligné.
- Finalement, les Préposés avaient émis des remarques spécifiques à certaines dispositions du projet, reprenant pour la plupart les suggestions susmentionnées et qui se lisaient comme suit : "*Les art. 6 litt. c et 7 du projet reposent sur le consentement de la personne concernée. Un consentement général ne saurait être admissible et doit être évité. Nous serions d'avis qu'il conviendrait d'ajouter une disposition sur les exigences relatives à un consentement valable (forme, limité à une prestation spécifique et des documents spécifiques, validité du consentement limitée dans le temps ou jusqu'à la décision sur délivrance de la prestation…); Art 8: le citoyen doit savoir exactement pour quelles prestations (dans quelles finalités) il laisse les documents / données complémentaires à disposition. Ces éléments ne devraient pas pouvoir rester pour une durée indéterminée dans le coffre-fort numérique. Il sied également d'analyser les enjeux en matière de sécurité des données, car l'Etat reste responsable d'assurer la sécurité des données, puisqu'il met le service à disposition. Autre réflexion: qui est le responsable de traitement? La question des responsabilités n'est pas suffisamment réglée. Art. 13 – 14: des accès différenciés seront-ils prévus selon les institutions publiques ou toutes auront accès à l'ensemble des informations? Il semble que certaines informations ne sont pas nécessaires à toutes les autorités de sorte que le principe de la proportionnalité devrait conduire à parfois limiter l'accès (ex: numéro d'identification du conjoint). Art. 16 – 17: voir remarques ci-dessus concernant le consentement. Art. 20: qui arbitre en cas d'informations contradictoires? Qui est le responsable de traitement du référentiel cantonal?*".
- Ils avaient encore suggéré qu'une analyse d'impact soit réalisée, bien que la nLIPAD, dont l'art. 37B prévoit cette hypothèse, ne soit pas encore en vigueur. Une telle analyse a été jointe au projet présentement soumis.

L'exposé des motifs joint à la dernière version du projet apporte des précisions en lien avec les deux objectifs du projet.

S'agissant de la simplification des démarches administratives pour les usagers et usagères, elle repose sur le principe du once only. Le projet propose une mise en œuvre de ce concept, "*allant de l'enregistrement des données de base des personnes dans des*

référentiels unifiés, à la possibilité, pour les usagères, les usagers, dont les entreprises, de consentir à la réutilisation des documents et données fournis ou produits par les services, et de donner mandat au service requis de délivrer la prestation (principale) de quérir lui-même des documents, prestations (accessoires) ou données préalables nécessaires auprès d'autres services de l'administration cantonale" (p. 28). Les domaines et prestations prioritaires seront définis par le Conseil d'Etat. Par ailleurs, les "données métier" (par opposition aux données personnelles de référence), ne doivent pas être partagées auprès d'autres services, sauf demande expresse de l'usager ou de l'usagère, qui souhaite bénéficier d'autres prestations de manière facilitée. En effet, "*Par exemple, 60% des pièces justificatives fournies pour la déclaration d'impôts des personnes physiques sont similaires à celles nécessaires pour une demande de subside au service de l'assurance-maladie (SAM). Un second exemple montre que 100% des pièces justificatives demandées par l'office cantonal des poursuites (OCP) dans le cadre de l'exécution d'une saisie, afin de déterminer le minimum vital du débiteur, sont déjà en possession du service des prestations complémentaires (SPC), si la personne a fait la demande de prestation. Actuellement, la personne est tenue de fournir deux fois le dossier à deux offices différents. Avec l'objectif de simplification administrative, la personne peut tenir à disposition, une seule fois (sous réserve des périodicités auxquelles ces pièces doivent être produites auprès de ces autorités), des données et documents auprès de plusieurs services dont elle a librement déterminé le périmètre*" (p. 30).

Le deuxième objectif du projet a trait à la dotation de référentiels de données de base pour les personnes physiques et morales, largement accessibles par les institutions publiques. En effet, les adresses dans la base de données CALVIN mise à disposition par l'OCPM ne sont pas toujours fiables (par exemple, 10% des personnes ne satisfont pas à leur obligation d'annonce de changement de domicile; difficulté pour des services étatiques d'établir le domicile d'un administré; selon l'Office fédéral de la statistique, au 31 décembre 2022, la proportion des ménages non plausibles dans le canton de Genève s'élevait à 1% contre moins de 0,5% dans l'ensemble des autres cantons). Ainsi, "*pour doter les institutions publiques du canton, dont certaines entités de droit privé chargées de tâches de droit public, de données de base fiables, le présent projet prévoit d'instituer deux référentiels relatifs aux données de référence des personnes, le premier pour les personnes physiques (art. 13), le second pour les personnes morales et les entreprises (art. 14). Ces référentiels ne contiennent que des données de base d'identification des personnes, qui sont univoques, et autant que possible actuelles et exactes, ainsi que des données nécessaires à la facilitation des interactions avec les administrations, telles les numéros de téléphone et les adresses électroniques, la mention de l'éventuel représentant légal ou le représentant désigné par la personne, de même que le conjoint ou la conjointe, le ou la partenaire enregistrée (via le numéro d'identification), qui sont en mesure de se représenter mutuellement au titre de l'union conjugale pour les besoins courants de la famille pendant la vie commune (art. 166 CC)*" (p. 34). Ces référentiels seront accessibles à l'ensemble des institutions publiques du canton, ainsi qu'à des privés chargés de tâches publiques. Le projet prévoit en outre que "*les données personnelles de référence contenues dans les applications métier des institutions publiques doivent alimenter autant que nécessaire les référentiels cantonaux, sauf si une loi (fédérale ou cantonale) ou un règlement l'interdit, cela tant à l'initialisation des référentiels que lors de leur mise à jour, et gratuitement (art. 21)*" (p. 36). De plus, "*le signalement de données erronées interviendra par un flux numérique retour à destination des référentiels cantonaux des données de référence, dont les autorités responsables (art. 25 al. 1) seront respectivement l'OCPM s'agissant des personnes physiques et l'OCIRT pour les personnes morales et les entreprises*" (p. 37). Finalement, "*dans la mesure où l'établissement de la réalité de certaines données peut s'avérer complexe, telle celle du domicile comme relevé par la représentante de l'OCPM, le présent projet prévoit la possibilité pour les institutions publiques de pouvoir échanger spontanément ou sur requête avec les autorités responsables visées à l'article 25, alinéa 1, aux seules fins de garantir l'unicité, l'exactitude, l'actualité et la complétude des données de base des personnes, à moins que cette*

information ne soit contraire à une loi (fédérale ou cantonale) ou à un règlement (art. 23). En dehors de ces échanges portant sur les données de référence des personnes, et des éventuels éléments et motifs qui amèneraient à devoir procéder à leur correction et mise à jour (déménagement, décès, séparation, etc.), les institutions publiques respectent le secret de fonction et les autres secrets qualifiés et secrets professionnels" (p. 38).

L'avis relatif au présent projet est sollicité, idéalement, pour le 24 juin 2025.

L'ensemble du projet ayant trait à des questions de protection des données, les articles seront repris en tant que de besoin dans l'appréciation. De même, les éléments de l'analyse d'impact qui appellent des commentaires seront repris dans l'appréciation.

2. Les dispositions de la LIPAD

En édictant la loi sur l'information du public, l'accès aux documents et la protection des données, du 5 octobre 2001 (LIPAD; RSGe A 2 08), entrée en vigueur le 1er mars 2002, le législateur a érigé la transparence au rang de principe aux fins de renforcer tant la démocratie que le contrôle de l'administration, valoriser l'activité étatique et favoriser la mise en œuvre des politiques publiques. S'agissant de son volet relatif à l'accès aux documents en mains des institutions publiques, la LIPAD a ainsi pour "*but de favoriser la libre information de l'opinion et la participation à la vie publique*" (art. 1 al. 2 litt. a LIPAD).

En 2008, la loi a fait l'objet d'une révision importante. Au volet relatif à la transparence, le domaine de la protection des données personnelles a été ajouté.

A ce titre, la loi a pour but de "*protéger les droits fondamentaux des personnes physiques ou morales de droit privé quant aux données personnelles les concernant*" (art. 1 al. 2 litt. b LIPAD). Dans cette autre matière, la loi "*tend d'abord à favoriser le confinement des informations susceptibles de porter atteinte à la personnalité*" (Rapport de la Commission judiciaire et de la police chargée d'étudier le projet de loi du Conseil d'Etat sur la protection des données personnelles (LPDP) (A 2 12) (PL 9870-A, p. 5). Ce volet est entré en vigueur le 1er janvier 2010.

Le 3 mai 2024, le Grand conseil a adopté la loi modifiant la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) (L 13347)[1] qui apporte des modifications à la LIPAD, principalement en matière de protection des données. Cette nouvelle version de la loi (nLIPAD) n'est à ce jour pas en vigueur, mais il est pertinent de l'évoquer, parallèlement aux dispositions actuellement en vigueur, afin de permettre l'appréciation du projet de loi présentement soumis.

Par données personnelles, il faut comprendre "toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable" (art. 4 litt. a LIPAD).

Par données personnelles sensibles, la loi vise les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques, syndicales ou culturelles ; la santé, la sphère intime ou l'appartenance ethnique ; des mesures d'aide sociale ; des poursuites ou sanctions pénales ou administratives (art. 4 litt. b LIPAD). L'art. 4 litt. b nLIPAD ajoute les données génétiques, ainsi que les données biométriques identifiant une personne physique de façon unique.

La LIPAD énonce un certain nombre de principes généraux régissant la collecte et le traitement des données personnelles (art. 35 à 40 LIPAD). Ces principes se retrouvent dans la nLIPAD (art. 35 – 36 nLIPAD).

- Base légale (art. 35 LIPAD; art. 36 nLIPAD)

Le traitement de données personnelles ne peut se faire que si l'accomplissement des tâches légales de l'institution publique le rend nécessaire. Quant aux données personnelles sensibles ou aux profils de la personnalité, ils ne peuvent être traités que si une loi définit

[1] https://ge.ch/grandconseil/data/loisvotee/L13347.pdf

clairement la tâche considérée et si le traitement en question est absolument indispensable à l'accomplissement de cette tâche ou s'il est nécessaire et intervient avec le consentement explicite, libre et éclairé de la personne concernée.

La nLIPAD prévoit à son art. 36 que 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. S'agissant des traitements de données personnelles sensibles et des activités de profilage, selon l'art. 36 al. 2 nLIPAD, une loi au sens formel doit le prévoir expressément ou le traitement doit être indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel. En dérogation aux al. 1 et 2, l'art. 36 al. 3 nLIPAD prévoit que des données personnelles, y compris sensibles, peuvent être traitées notamment si la personne concernée a consenti au traitement en l'espèce. Le consentement doit pouvoir être démontré par le responsable de traitement, n'est valable que s'il est informé et exprimé concernant un ou plusieurs traitements déterminés (al. 4) et est révocable en tout temps et sans motifs (al. 5).

- Bonne foi (art. 38 LIPAD; art. 35 al. 2 nLIPAD)

Il n'est pas permis de collecter des données personnelles sans que la personne concernée en ait connaissance, ni contre son gré. Quiconque trompe la personne concernée lors de la collecte des données – par exemple en collectant les données sous une fausse identité ou en donnant de fausses indications sur le but du traitement – viole le principe de la bonne foi. Il agit également contrairement à ce principe s'il collecte des données personnelles de manière cachée.

- Proportionnalité (art. 36 LIPAD; art. 35 al.2 nLIPAD)

En vertu du principe de la proportionnalité, seules les données qui sont nécessaires et qui sont aptes à atteindre l'objectif fixé peuvent être traitées. Il convient donc toujours de peser les intérêts en jeu entre le but du traitement et l'atteinte à la vie privée de la personne concernée en se demandant s'il n'existe pas un moyen moins invasif permettant d'atteindre l'objectif poursuivi.

- Finalité (art. 35 al. 1 LIPAD; art. 35 al. 1 nLIPAD)

Conformément au principe de finalité, les données collectées ne peuvent être traitées que pour atteindre un but légitime qui a été communiqué lors de leur collecte, qui découle des circonstances ou qui est prévu par la loi. Les données collectées n'ont ensuite pas à être utilisées à d'autres fins, par exemple commerciales.

- Reconnaissabilité de la collecte (art. 38 LIPAD; art. 35 al. 3 nLIPAD)

La collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée. Cette exigence de reconnaissabilité constitue une concrétisation du principe de la bonne foi et augmente la transparence d'un traitement de données. Cette disposition implique que, selon le cours ordinaire des choses, la personne concernée doit pouvoir percevoir que des données la concernant sont ou vont éventuellement être collectées (principe de prévisibilité). Elle doit pouvoir connaître ou identifier la ou les finalités du traitement, soit que celles-ci lui sont indiquées à la collecte ou qu'elles découlent des circonstances.

- Exactitude (art. 36 LIPAD; art. 35 al. 5 et 6 nLIPAD)

Quiconque traite des données personnelles doit s'assurer de l'exactitude de ces dernières. Ce terme signifie également que les données doivent être complètes et aussi actuelles que les circonstances le permettent. La personne concernée peut demander la rectification de données inexactes. L'art. 36 al. 2 (art. 35 al. 6 nLIPAD) prévoit que lorsqu'une institution publique constate que des données personnelles qu'une autre institution lui a communiquées en vertu de l'art. 39 al. 1, sont inexactes, incomplètes ou obsolètes, elle en informe cette dernière, à moins que cette information ne soit contraire à une loi ou à un règlement.

- Sécurité des données (art. 37 LIPAD; art. 37A nLIPAD)

Le principe de sécurité exige non seulement que les données personnelles soient protégées contre tout traitement illicite et tenues confidentielles, mais également que l'institution en charge de leur traitement s'assure que les données personnelles ne soient pas perdues ou détruites par erreur.

- Destruction des données (art. 40 LIPAD; art. 35 al. 4 nLIPAD)

Les institutions publiques détruisent ou rendent anonymes les données personnelles dont elles n'ont plus besoin pour accomplir leurs tâches légales, dans la mesure où ces données ne doivent pas être conservées en vertu d'une autre loi.

L'art. 39 LIPAD traite de la communication des données personnelles, en fonction du destinataire. Il prévoit ce qui suit s'agissant de la communication de données personnelles à une autre institution publique soumise à la LIPAD:

[1] Sans préjudice, le cas échéant, de son devoir de renseigner les instances hiérarchiques supérieures dont elle dépend, une institution publique ne peut communiquer des données personnelles en son sein ou à une autre institution publique que si, cumulativement :

a) l'institution requérante démontre que le traitement qu'elle entend faire des données sollicitées satisfait aux exigences prévues aux articles 35 à 38;

b) la communication des données considérées n'est pas contraire à une loi ou un règlement.

[2] L'organe requis est tenu de s'assurer du respect des conditions posées à l'alinéa 1 et, une fois la communication effectuée, d'en informer le responsable sous la surveillance duquel il est placé, à moins que le droit de procéder à cette communication ne résulte déjà explicitement d'une loi ou d'un règlement.

[3] Les institutions publiques communiquent aux autorités judiciaires les données personnelles que celles-ci sollicitent aux fins de trancher les causes dont elles sont saisies ou de remplir les tâches de surveillance dont elles sont investies, sauf si le secret de fonction ou un autre secret protégé par la loi s'y oppose.

Cette dernière disposition ne connaît pas de modification significative dans la nLIPAD.

3. La loi sur l'harmonisation des registres (LHR)

La loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes (loi sur l'harmonisation de registres; LHR; RS 431.02) vise à simplifier la collecte de données à des fins statistiques par l'harmonisation des registres officiels de personnes et l'échange, prévu par la loi, de données personnelles entre les registres (art. 1 al. 1).

Son article 2 a trait au champ d'application de la loi. Il prévoit qu'elle s'applique, s'agissant des cantons, au registre informatisé de l'état civil (Infostar), aux registres cantonaux et communaux des habitants, ainsi qu'aux registres cantonaux et communaux des électeurs, lorsque ces registres servent aux votations populaires et aux élections du Conseil national.

Par registre des habitants, la loi vise le registre, tenu de manière informatisée ou manuelle par le canton ou la commune, dans lequel sont inscrites toutes les personnes qui y sont établies ou en séjour (art. 3 litt. a).

Selon l'art. 5, "*Les registres doivent contenir des données actuelles, exactes et complètes par rapport à l'ensemble des personnes visées*."

L'art. 6 prévoit que: "*Les registres des habitants contiennent au minimum, pour chaque personne établie ou en séjour, les données relatives aux identificateurs et aux caractères suivants:*

a. numéro AVS12 au sens de l'art. 50c de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS);

b. numéro attribué par l'office à la commune et nom officiel de la commune;

c. identificateur de bâtiment selon le Registre fédéral des bâtiments et des logements (RegBL) de l'office;

d. identificateur de logement selon le RegBL, ménage dont la personne est membre et catégorie de ménage;

e. nom officiel de la personne et autres noms enregistrés à l'état civil;

f. totalité des prénoms cités dans l'ordre exact;

g. adresse et adresse postale, y compris le numéro postal d'acheminement et le lieu;

h. date de naissance et lieu de naissance;

i. lieux d'origine, si la personne est de nationalité suisse;

j. sexe;

k. état civil;

l. appartenance à une communauté religieuse reconnue de droit public ou reconnue d'une autre manière par le canton;

m. nationalité;

n. type d'autorisation, si la personne est de nationalité étrangère;

o. établissement ou séjour dans la commune;

p. commune d'établissement ou commune de séjour;

q. en cas d'arrivée: date, commune ou État de provenance;

r. en cas de départ: date, commune ou État de destination;

s. en cas de déménagement dans la commune: date;

t. droit de vote et éligibilité aux niveaux fédéral, cantonal et communal;

u. date de décès".

4. Appréciation

Le projet de loi est divisé en 5 chapitres :

- Chapitre I: Dispositions générales (art. 1 – 5)
- Chapitre II: Simplification administrative (art. 6 – 12)
- Chapitre III: Référentiels cantonaux des personnes physiques, des personnes morales et des entreprises (art. 13-15)
- Chapitre IV: Protection, sécurité et gouvernance des données personnelles (art. 16 – 25)
- Chapitre V: Dispositions finales et transitoires (art. 26 – 27).

Ces chapitres feront l'objet d'une appréciation qui sera suivie de quelques remarques liées à l'analyse d'impact et aux question relatives à la sécurité des données.

Les dispositions générales:

L'objet et les buts de la loi sont définis à ses art. 1 et 2. S'agissant de l'échange de données de base entre les institutions publiques et les autorités responsables des référentiels, l'art. 2 litt. e précise la finalité de cet échange, qui intervient "*aux seules fins de garantir l'unicité, l'exactitude, l'actualité et la complétude de leurs données*". Au vu des multiples bases de données concernées par le projet, cette limitation de la finalité est une précision utile.

Les Préposés relèvent que l'art. 3 al. 2 litt. c prévoit qu'ils soient consultés dans le cadre de la coordination entre la loi présentement soumise et la LIPAD notamment. Ils remercient le DF de les intégrer au processus.

L'art. 4 a trait au champ d'application de la loi. Les Préposés constatent qu'il est extrêmement large, même sensiblement plus large que celui de la LIPAD, dans son volet protection des données.

S'agissant des définitions, l'art. 5 al. 1 et 2 renvoie à diverses lois avec lesquelles la loi doit se coordonner. Comme le mentionne l'exposé des motifs (p. 42), cela permet une bonne cohérence entre les définitions prévues par différentes lois, ce qui est nécessaire. L'alinéa 3 définit un certain nombre de notions qui sont au cœur du présent projet de loi. Les Préposés relèvent que la notion de "données personnelles complémentaires" vise potentiellement toutes les données personnelles, sensibles ou non, qui ne sont pas des données personnelles de référence.

Il découle de ce qui précède que le projet de loi constitue une base légale qui, à terme, pourrait couvrir l'intégralité des activités de l'administration et des institutions publiques genevoises, voire même de privés effectuant des tâches publiques. Ainsi, les traitements pourraient être potentiellement extrêmement intrusifs au niveau de la sphère privée, malgré le consentement des citoyens. C'est pourquoi, il importe que lesdits traitements soient clairement encadrés, que le consentement soit spécifique, que l'utilisation du coffre-fort numérique reste facultative pour les usagères et les usagers et que la gestion des droits d'accès soit régulée avec soin. Le cycle de vie des données importe également, notamment au regard de la proportionnalité. Par ailleurs, la question de la sécurité des données est centrale dans un tel projet, tant les conséquences d'une usurpation d'identité pourraient être dommageables. Ces éléments seront détaillés en tant que de besoin ci-dessous.

Le chapitre II sur la *simplification administrative* est composé des art. 6 à 12.

L'art. 6 consacre le principe du "once-only". A cet égard, les Préposés se demandent si l'art. 6 al. 1 litt. c ne devrait pas déjà mentionner que la collecte des données et documents nécessaires auprès d'autres institutions publiques intervient uniquement si l'usager le souhaite (caractère facultatif); la notion de consentement prévue à l'art. 7 demeurerait, précisant cette notion et ses exigences. En effet, le recours à cette possibilité de collecte "automatique" par les institutions publiques doit rester facultative pour les usagers. Peut-être conviendrait-il de le préciser.

L'art. 7 précise la nécessité d'un consentement préalable et en règle les modalités, notamment en renvoyant aux dispositions topiques de la nLIPAD sur le consentement, coordination entre les deux lois que les Préposés saluent. En effet, ce renvoi implique que les exigences de l'art. 36 al. 4 et 5 nLIPAD doivent être respectées: le consentement n'est valable que s'il porte sur un ou plusieurs traitements déterminés et qu'il est donné après que la personne concernée a été dûment informée. Le retrait du consentement est possible en tout temps.

L'art. 9 qui a trait aux émoluments prévoit que "*Dans la mesure où le cadre légal n'y fait pas obstacle et l'organisation et l'environnement de travail le permettent, les institutions publiques cantonales visées à l'article 4, alinéa 1, requises de délivrer une prestation, impliquant la délivrance préalable d'autres prestations d'autres institutions publiques cantonales soumises à émolument ou frais, se chargent de réclamer le paiement du montant total dû par l'usagère ou l'usager*". Cette disposition soulève une question plus large et récurrente dans le projet de loi présentement soumis. A plusieurs reprises, il est en effet fait référence au "cadre légal" qui pourrait s'opposer à certaines communications de données (voir également ci-dessous ad art. 13 al. 2 et 21 al.1), sans que ce cadre ne soit précisé pour autant. Si la question des secrets ou des devoirs de confidentialité expressément prévus par des lois spéciales ou par des règlements apparaissent couverts par cette formulation, la question est moins claire concernant les données personnelles sensibles. Cela mériterait d'être clarifié. Cette question est ici moins problématique, puisque les Préposés comprennent que cet émolument global ne peut intervenir que dans les cas où l'usager ou l'usagère a expressément donné son consentement à la quête des données personnelles et documents auprès d'autres institutions publiques, conformément à l'art. 7 du projet. Si tel est le cas, cette disposition semble conforme aux exigences de protection des données, bien que cela puisse impliquer qu'une institution publique effectue potentiellement une mission qui ne lui est pas conférée par la loi et qui n'entre pas dans ses tâches. L'on peut se demander si cela n'entre pas en contradiction avec l'art. 11 du projet (voir ci-dessous).

Les art. 10 à 12 régissent le "coffre-fort numérique", à savoir "*la plateforme électronique centralisée chargée de collecter, gérer et mettre à disposition des documents et des données personnelles complémentaires auprès d'institutions publiques selon les modalités définies par les usagers et les usagères*" (art. 5 al. 3 litt. d).

Comme déjà mentionné, les Préposés insistent sur le caractère large des documents et données personnelles, y compris, sensibles qui peuvent y figurer, tout comme le nombre potentiel extrêmement grand d'institutions qui pourraient, à terme, se voir octroyer des accès, dans les limites de leur mission évidemment. Les enjeux en termes de protection des données sont donc centraux, notamment en termes de sécurité des données.

Comme l'indique l'exposé des motifs, l'art. 10 "*décrit les modalités de mise à disposition de documents et de données personnelles complémentaires à une ou plusieurs institutions publiques, si les usagères et les usagers le souhaitent et selon les modalités qu'elles ou ils ont définies*" (p. 43). Cette disposition donne une grande place à la volonté des usagères et usagers, dans les limites de leurs besoins administratifs. Les précisions apportées par l'exposé des motifs sont bienvenues: les modalités de partage doivent porter sur des documents individualisés (par exemple : une carte d'identité, un extrait du registre des poursuites) ou des données personnelles déterminées. "*Les usagères et usagers déterminent les institutions auprès desquelles elles ou ils entendent diffuser les documents et données personnelles complémentaires. Toutefois, pour des motifs de protection des données (proportionnalité, finalité et « reconnaissabilité », cf. art. 35 al. 2 et 3 LIPAD, loi 13347), le consentement de partage des documents et données à une institution tierce n'est pas suffisant, car il doit porter spécifiquement sur une ou des prestations déterminées (par ex. : une autorisation de construire, l'obtention de prestations complémentaires) ou, du moins sur des finalités déterminées et reconnaissables*" (p. 43). Les Préposés saluent également le fait que des dispositions prévoient des limites de conservation des documents. Ils y reviendront ci-dessous en lien avec l'art. 18 du projet.

S'agissant de l'accès aux documents et aux données personnelles complémentaires, il est prévu par l'art. 11 du projet. Cette disposition soumet l'accès à la double condition du consentement donné par les usagères et les usagers et de la nécessité de l'information pour l'accomplissement des tâches légales de l'institution. Elle permet de respecter les exigences de licéité en matière de protection des données, puisque seules les institutions publiques

ayant une base légale dans la loi qui régit leur activité pourront avoir accès aux données; elle garantit également le consentement de l'usager.

L'art. 12 régit la révocation du consentement. Comme l'indique l'exposé des motifs (p. 44), cette disposition est le corollaire des art. 10 et 11 du projet, puisqu'elle prévoit la faculté de révoquer en tout temps et sans motif le partage des données et documents qu'ils ont mis à disposition dans le coffre-fort numérique. Il conviendra toutefois d'attirer l'attention des citoyens sur le fait que le retrait du consentement ne vaut que pour l'avenir. En effet, conformément à ce que prévoit l'art. 12 al. 3, une fois fournis pour une prestation / institution spécifique, les données complémentaires et documents vont figurer dans les applications métier desdites institutions. Pour que l'information du citoyen soit complète, il devra être conscient de cette conservation, même s'il retire ultérieurement les données complémentaires / documents du coffre-fort numérique.

Les Préposés relèvent finalement avec satisfaction que les remarques qu'ils avaient émises par courriel du 28 octobre 2024 ont été prises en considération (notamment la précision des exigences relative à un consentement valable; les accès différenciés; la définition d'un responsable de traitement).

Finalement, les Préposés insistent une fois encore sur les enjeux liés à la sécurité des données, tant les conséquences de violation des données seraient dommageables. Ils relèvent que la mise sur pied technique du système prévu par le projet de loi s'avère très complexe.

Le chapitre III concerne les *référentiels cantonaux des personnes physiques, des personnes morales et des entreprises (art. 13-15)*.

Les Préposés relèvent qu'en terme de champ d'application, il s'agit de référentiels extrêmement larges, puisqu'ils sont constitués de l'ensemble des données personnelles de référence des personnes "identifiées" auprès des institutions publiques visées à l'art. 4 (art. 13 al. 2 et 14 al. 2). Cela comprend ainsi le Conseil d'État, le pouvoir judiciaire et son administration, l'administration cantonale, les communes, leurs administrations, ainsi que les groupements intercommunaux, les institutions, établissements et corporations de droit public cantonaux et communaux, ainsi que leurs administrations et, sur désignation du Conseil d'Etat, les personnes physiques ou morales et organismes chargés de remplir des tâches de droit public cantonal ou communal, dans les limites de l'accomplissement desdites tâches.

Par ailleurs, les art. 13 al. 2, 2ème phrase et 14 al. 2, 2ème phrase prévoient que les référentiels sont alimentés par les bases de données des applications métier de ces institutions, sauf si une loi ou un règlement l'interdit, et sont mis à jour sous la responsabilité de l'autorité prévue à l'art. 25 al. 1. Cette dernière disposition prévoit que c'est le Conseil d'État qui désigne ladite autorité qui sera responsable de traitement.

Les Préposés comprennent donc que si une personne physique / morale / entreprise figure dans la base de données métier d'une des institutions susmentionnées, elle figurera dans le référentiel des personnes physiques, respectivement des personnes morales et des entreprises. Si cette compréhension s'avère exacte, le critère de rattachement pour figurer dans le référentiel cantonal est très large et va bien au-delà des objectifs de la LHR, à laquelle le projet de loi se réfère. En effet, cela pourrait avoir pour conséquence que si un témoin domicilié hors canton figure dans la base de données du Pouvoir judiciaire, il pourrait se retrouver dans le référentiel cantonal des personnes physiques. De même, un patient étranger soigné aux HUG pourrait figurer dans le référentiel cantonal des personnes physiques. Le secret médical empêcherait probablement que le deuxième cas de figure se produise. La notion de "personnes *identifiées* auprès des institutions publiques visées à l'art. 4" apparaît, à lui seul, comme un critère de rattachement trop large. Malgré les cautèles

prévues par les limitations instaurées par les droits d'accès ou encore les limitations légales ou réglementaires à la communication de données (abordées ci-dessous), le principe de finalité apparaît difficile à respecter, lorsque le lien entre une personne concernée et Genève est aussi ténu. Les Préposés suggèrent de préciser et réduire ce critère de rattachement.

Un autre élément qui suscite une certaine crainte de la part des Préposés a trait au fait que les référentiels sont alimentés par les bases de données des applications métier des institutions. S'ils ne s'y opposent pas sur le principe, car ils comprennent la nécessité de pouvoir échanger sur des informations potentiellement contradictoires concernant des domiciliations ou autres données de base, ces échanges peuvent intrinsèquement amener à la divulgation de données sensibles. En effet, toutes les données de base versées par une institution comme l'Hospice général par exemple divulguent intrinsèquement une donnée sensible qui est celle de bénéficier de l'aide sociale. Le fait que l'art. 2 mentionne que le référentiel est alimenté par les bases de données des applications métier des institutions "*sauf si une loi ou un règlement l'interdit*" est une limite aux échanges automatiques dans certains cas; toutefois, sa portée n'apparaît pas suffisamment précise (tout comme celle de l'art. 21 al. 1 du projet) et elle n'est pas précisée à la lecture de l'exposé des motifs. En effet, il est difficile de déterminer si le cas susmentionné serait visé par cette interdiction ou si l'ensemble des données de base de l'Hospice général pourraient alimenter le référentiel. Les principes de finalité et de proportionnalité exigent, selon les Préposés, que seules les données identifiées comme contradictoires par les institutions autres que celle qui est responsable de traitement des référentiels cantonaux soient communiquées au référentiel cantonal (ce que prévoient les art. 20 al. 2 et 22 du projet). Ils suggèrent donc que ces éléments soient clarifiés, à tout le moins dans l'exposé des motifs. Par ailleurs, les citoyens doivent pouvoir comprendre quelles bases de données métier seraient concernées et automatiquement versées dans le référentiel. Les base de données-métier qui portent par définition sur des données personnelles sensibles devraient être exclues et la communication ne devrait intervenir qu'au cas par cas, en cas de données contradictoires.

L'art. 13 al. 3 litt. a prévoit que "*les données de base de l'identité*" figurent dans le référentiel. Cette notion de "données de base" apparaît à plusieurs reprises dans le projet de loi. Elle mériterait d'être définie.

Les Préposés saluent les art. 13 al. 4 et 14 al. 4, qui prévoient que le Conseil d'Etat établit par voie réglementaire le cercle des institutions publiques ayant accès au référentiel et le niveau d'accès aux données personnelles de référence en fonction de la nécessité de traitement. Ces dispositions permettent de respecter les exigences de protection des données, en particulier la proportionnalité. En pratique, la mise en œuvre de la gestion des droits d'accès constituera un enjeu considérable. Les Préposés saluent également le fait que les données qui figurent dans les référentiels cantonaux soient listées exhaustivement à l'alinéa 3.

Finalement, les Préposés saluent l'art. 15 du projet qui prévoit que l'accès aux données personnelles de référence est réservé aux institutions publiques, seulement dans la mesure où leur consultation est nécessaire à la délivrance des prestations et s'inscrit dans l'accomplissement d'une tâche légale. Ils saluent également l'alinéa 2 qui rappelle expressément les droits des citoyens en matière d'accès à leurs propres données personnelles. Ces dispositions rappellent le cadre imposé par la LIPAD.

Le chapitre IV a trait à la *protection, sécurité et gouvernance des données personnelles.*

L'art. 16 du projet rappelle les devoirs du responsable de traitement. Il n'appelle pas de commentaire particulier. Il s'agit d'une application des dispositions relatives à la sécurité des données prévues par la LIPAD. La question de savoir si leur rappel est nécessaire, vu le caractère transversal de la LIPAD, peut se poser. Par contre, au vu des enjeux d'ores et déjà

identifiés en matière de sécurité des données, la mise en application pratique de la loi risque de s'avérer délicate.

L'art. 17 prévoit la journalisation des opérations et garantit ainsi l'usage conforme de l'accès aux données.

L'art. 18 a le mérite de prendre en compte le cycle de vie des données. Il prévoit, s'agissant du coffre-fort numérique, que le détail sera réglé par voie réglementaire, ce qui apparaît conforme aux règles de protection des données.

L'art. 21 a trait à la communication de données personnelles de référence par les institutions publiques aux autorités responsables des référentiels cantonaux. Comme cela a été mentionné ci-dessus au sujet des art. 13 al. 2 et 14 al. 2, et pour les mêmes motifs, l'art. 21 al. 1 mériterait d'être précisé. L'art. 21 al. 2, en tant qu'il représente une base légale spécifique concernant les données de l'administration fiscale, n'appelle pas de commentaires. En effet, la licéité et la transparence de la communication sont assurées.

L'art. 22 qui a trait au signalement de données personnelles erronées reprend une règle déjà présente dans la LIPAD, à savoir l'art. 36 al. 2. Cette disposition respecte les exigences de proportionnalité, contrairement à ce que prévoit l'art. 21 al.1 du projet.

L'art. 24 prévoit la possibilité d'utiliser les numéros AVS et IDE de manière systématique, suite à l'introduction de l'art. 153b LAVS. Comme l'exposé des motifs l'indique, la disposition "*limite expressément leur utilisation aux seules fins de l'identification sûre et univoque des personnes, d'assurer un taux d'exactitude des données le plus élevé possible et d'un échange automatique de données en cas de changement intervenu. Cette disposition sert par ailleurs de base légale cantonale à l'utilisation des numéros AVS et IDE par les autres institutions publiques visées à l'article 4, alinéa 2, lettre c, que sont, sur désignation du Conseil d'Etat, les personnes physiques ou morales et organismes chargés de remplir des tâches de droit public cantonal ou communal (comme par exemple les EMS et les EPH), qui requièrent une base légale cantonale spécifique*" (p. 48). Les Préposés saluent que les finalités soient expressément mentionnées à l'art. 24 al. 1, tout comme le fait que l'al. 2 prohibe expressément toute autre utilisation.

L'art. 25 al. 1 prévoit que le Conseil d'Etat désigne l'autorité ou les autorités chargées de la tenue et mise à jour des référentiels cantonaux, autorités qui sont également la ou les responsables de traitement au sens de la nLIPAD. L'alinéa 2 liste les compétences desdites autorités. Les Préposés saluent le fait qu'une autorité (ou plusieurs) soit clairement définie comme responsable de traitement. En cas de traitement conjoint, les obligations respectives de chaque responsable de traitement devront être définies de manière transparente (art. 36B nLIPAD). Cette précision vaut également pour l'art. 25 al. 3 et 4.

Au sujet de l'analyse d'impact

Les Préposés remercient le responsable LIPAD du DF d'avoir effectué une analyse d'impact, alors que la version actuellement en vigueur de la LIPAD ne l'exigeait pas encore.

Ils considèrent en effet que si la nLIPAD était en vigueur, le projet envisagé aurait nécessité une analyse d'impact au vu des éléments suivants:

- étendue du champ d'application de la loi
- caractère non délimité des données personnelles, y compris sensibles, et documents pouvant figurer dans le coffre-fort numérique
- projet de loi qui donne une base légale à un potentiel traitement de données personnelles sensibles à grande échelle
- interconnexion de différentes bases de données

- données personnelles accessibles en ligne selon le principe de self-service
- communication systématique de données personnelles

Ces éléments constituent à notre sens suffisamment d'indices pour qu'une analyse d'impact soit nécessaire. En effet, les atteintes potentielles aux droits fondamentaux des personnes concernées sont importantes, en particulier avec le coffre-fort numérique : de nombreux pans de la sphère privée des citoyens pourraient y figurer (santé, prestations sociales, situation fiscale…). Une violation des données ou une usurpation d'identité pourraient avoir des conséquences graves (ce qui est par ailleurs relevé dans l'analyse d'impact effectuée).

Cette analyse a ainsi le mérite de mettre en évidence les risques liés à la sécurité des données. Toutefois, les informations communiquées pour remédier à ces risques sont à ce stade peu détaillées et permettent difficilement d'évaluer le risque résiduel.

Les Préposés relèvent ce qui suit, sur la base des quelques informations fournies concernant les risques liés à la sécurité de l'information:

- Aucun enjeu lié au cloud ne devrait se poser, puisque les données sont gérées en local;
- La question de la sécurisation des échanges de données entre les bases locales et les bases de données de référence se pose notamment pour les institutions disposant d'un réseau informatique séparé (non géré par l'OCSIN). Un schéma des flux de données et des mesures de sécurité afférentes serait utile à la compréhension des risques et des enjeux.

Les Préposés sont d'avis que l'analyse d'impact devrait être complétée une fois que le DF aura une vision plus précise du fonctionnement technique envisagé. En effet, à ce stade, il est difficile d'estimer les risques, les risques résiduels et les mesures pour y pallier, car l'analyse manque quelque peu d'éléments techniques concrets. Cela devra donc faire l'objet d'un examen ultérieur.

* * * * * *

Les Préposés remercient le DF de les avoir consultés, de prendre en considération les remarques susmentionnées et se tiennent à disposition pour tout renseignement complémentaire.

Joséphine Boillat
Préposée adjointe

Stéphane Werly
Préposé cantonal