Date de dépôt : 15 mars 2017

Réponse du Conseil d'Etat

à la question écrite urgente de Mme Salika Wenger : Quelle protection pour les données des citoyen-ne-s ?

Mesdames et
Messieurs les députés,

En date du 24 février 2017, le Grand Conseil a renvoyé au Conseil d'Etat une question écrite urgente qui a la teneur suivante :

La République et canton de Genève, les établissements autonomes de droit public, les fondations de droit public ainsi que l'Université de Genève et la HES-SO traitent au quotidien une masse considérable de données personnelles. La sécurité de ces dernières est régie par l'article 37 de la LIPAD qui indique dans son premier alinéa que « les données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques appropriées », dans son deuxième alinéa que « les institutions publiques prennent, par le biais de directives ainsi que de clauses statutaires ou contractuelles appropriées, les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent ou font traiter » et, enfin, dans son troisième alinéa que « les institutions publiques sont tenues de contrôler le respect des directives et clauses visées à l'alinéa 2 ». Partant de ces obligations en matière de protection des données personnelles, nous vous remercions de bien vouloir répondre aux questions suivantes :

1. ***Quelles directives, clauses statutaires ou contractuelles ont-elles été mises en place par les autorités pour la protection des données personnelles traitées par les services de l'Etat, les établissements autonomes de droit public, les fondations de droit public ainsi que l'Université de Genève et la HES-SO ?***

2. ***Des entreprises privées sont-elles amenées à traiter ou conserver des données personnelles collectées par les services de l'Etat, les établissements autonomes de droit public, les fondations de droit public ainsi que l'Université de Genève et la HES-SO ?***
3. ***Quelles directives, clauses statutaires ou contractuelles ont-elles été mises en place par les autorités pour la protection des données personnelles (conservation ou traitement) confiées par chacun des services de l'Etat, des établissements autonomes de droit public, des fondations de droit public ainsi que de l'Université de Genève ou de la HES-SO à des entreprises privées ?***
4. ***Lesquels des services de l'Etat, des établissements autonomes de droit public, des fondations de droit public, de l'Université de Genève et de la HES-SO sollicitent-ils les services d'entreprises privées en matière de traitement ou de conservation de données personnelles ?***
5. ***Quelles entreprises se chargent du traitement ou de la conservation de données personnelles collectées par des services de l'Etat, des établissements autonomes de droit public, des fondations de droit public, l'Université de Genève ou la HES-SO ?***
6. ***Quel est le coût global, ainsi que le coût par des services de l'Etat, des établissements autonomes de droit public, fondations de droit public, pour l'Université de Genève et la HES-SO de la délégation du traitement ou de la conservation de données personnelles à des entreprises privées ?***
7. ***Quel est le coût global, ainsi que le coût par entreprise, du traitement ou de la conservation des données personnelles confiées par des services de l'Etat, des établissements autonomes de droit public, des fondations de droit public, de l'Université de Genève et de la HES-SO ?***
8. ***Les entreprises privées traitant ou conservant des données personnelles pour les services de l'Etat, les établissements autonomes de droit public, les fondations de droit public ainsi que l'Université de Genève et la HES-SO ont-elles le droit de faire commerce de ces données d'une quelconque manière ?***

RÉPONSE DU CONSEIL D'ÉTAT

Le délai légal de réponse ne permet pas de fournir l'ensemble des informations consolidées demandées. C'est la raison pour laquelle la présente réponse se limitera à exposer le cadre juridique pertinent.

Introduction

Le Conseil d'Etat a adopté, le 8 février 2017, une modification du règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 21 décembre 2011 (A 2 08.01; RIPAD), – modification entrée en vigueur le 15 février 2017 – redéfinissant les règles relatives aux traitements transfrontières de données et au recours à des systèmes informatiques délocalisés ou dématérialisés (informatique en nuage) qui étaient prévues à l'ancien article 13, alinéas 5 et 6 RIPAD.

En effet, lors de l'adoption du RIPAD en 2011, le Conseil d'Etat avait délibérément choisi une solution cantonale restrictive, qui se distanciait du droit fédéral sur ces aspects et qui exigeait que le traitement de données personnelles s'effectue intégralement en Suisse. Cette dernière exigence a commencé, toutefois, à confronter les institutions publiques genevoises à des difficultés pratiques.

La solution offerte par le nouvel article 13A RIPAD adapte notre cadre réglementaire à la pratique fédérale et européenne, tout en limitant la communication de données vers des Etats assurant un niveau de protection adéquat. Il s'agit d'une solution intermédiaire entre l'interdiction totale qui prévalait depuis 2011 et la pratique relativement libérale de la réglementation fédérale. Plus précisément, la nouvelle réglementation fusionne en une seule et même disposition les questions de sous-traitance et de communication transfrontière de données (la communication transfrontière de données et l'informatique en nuage hors territoire suisse ne sont que des cas de sous-traitance à l'étranger). Elle vise ainsi à assurer une meilleure sécurité des données personnelles en encadrant précisément leur sous-traitance, ce qui n'était pas le cas jusqu'au 14 février 2017. De plus, elle ne prévoit pas que des conventions privées avec le sous-traitant ou que le consentement éclairé de l'intéressé puissent suffire à « guérir » un droit étranger n'offrant pas de protection adéquate.

Enfin, il convient de mentionner la loi sur l'administration en ligne, du 23 septembre 2016 (B 4 23; LAeL), non encore entrée en vigueur, qui prévoit, dans le cadre des prestations en lignes, différentes mesures de mise en conformité de la LIPAD, telles que la confidentialité dès la conception (« *privacy by design* ») ou la mise en œuvre d'instruments d'audit récurrents inspirés de ceux proposés par le Préposé fédéral à la protection des données et à la transparence (à savoir le Système de gestion en matière de protection des données ou « SGPD »), sans oublier la cartographie des échanges de données entre offices et l'examen rigoureux de leur licéité. Les questions posées visent deux problématiques différentes : le traitement des données personnelles par les services de l'Etat, les établissements autonomes de droit public, les fondations de droit public, l'Université de Genève et la HES-SO, d'une part, et la sous-traitance de telles données auprès d'entreprises privées, d'autre part.

Exigences en matière de protection des données personnelles traitées directement par l'autorité ou institution publique qui en a la responsabilité

L'article 37 de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (A 2 08; LIPAD), mentionné dans la question est précisé par l'article 13 RIPAD[1].

[1] L'article 13 RIPAD prévoit ce qui suit :

« **En général**

[1] Les institutions publiques prennent les mesures organisationnelles et techniques propres à assurer la sécurité des données personnelles.

[2] Pour l'administration cantonale, les mesures techniques et organisationnelles nécessaires à la sécurité des données personnelles sont définies notamment par le respect :

a) du règlement sur l'organisation et la gouvernance des systèmes d'information et de communication, du 26 juin 2013;

b) de l'article 23A, alinéa 5, du règlement d'application de la loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux, du 24 février 1999;

c) des directives approuvées par la commission de gouvernance des systèmes d'information et de communication;

d) des règles et mesures de sécurité édictées par les maîtres de fichiers, les responsables départementaux de la sécurité de l'information et la direction générale des systèmes d'information, sur la base des compétences définies par les règlements visés aux lettres a et b;

e) des prescriptions réglementaires et des directives en matière d'archivage.

Accès aux systèmes d'information

Cette disposition réglementaire fixe ainsi, à ses alinéas 1 et 3, les principes applicables au grand Etat, avec une exigence spécifique, pour les systèmes d'information, de répertoire des personnes y ayant accès; tandis que l'alinéa 2 ne vise que le petit Etat, en raison du champ d'application des normes citées.

Ce sont donc ces instruments-là qui sont mis en place.

A relever que l'absence de liste, à l'article 13 RIPAD, des risques spécifiques contre lesquels les données personnelles doivent être assurées – comme cela a été prévu au niveau fédéral à l'article 9 de l'ordonnance relative à la loi fédérale sur la protection des données, du 14 juin 1993 (RS 235.11; OLPD), – n'implique aucune lacune de protection de celles-ci, dans la mesure où le principe de l'article 37, alinéa 1 LIPAD indique déjà qu'elles doivent être protégées contre tout traitement illicite. Ce qui n'empêche, en revanche, nullement les institutions publiques de prévoir une liste interne identifiant les risques et les mesures permettant d'y remédier.

Le préposé cantonal à la protection des données et à la transparence (ci-après : PPDT) est chargé de centraliser les normes et directives qu'adoptent dans ce cadre les institutions visées à l'article 50 LIPAD (art. 56, al. 2, lettre c LIPAD) et rappelle, lors de ses visites aux institutions publiques, l'obligation qui leur incombe d'établir de tels actes. En revanche, excepté le cas de directives et clauses impliquant l'exploitation de ressources informatiques et le traitement de données personnelles, le PPDT n'est pas consulté pour les mesures prises par les institutions publiques[2].

S'agissant du petit Etat, l'administration s'est dotée d'un référentiel et de plusieurs directives relatives à la sécurité :

– PSI (politique de la sécurité de l'information, mentionnée expressément dans la LAeL);
– EGE-10-06 (Sécurité et usage des ressources informatiques et de communication de l'administration cantonale genevoise);
– EGE-10-07 (Directive sur l'usage conforme et le contrôle des ressources informatiques et de communication de l'administration cantonale);
– EGE-10-12 (Directive sur la classification des informations);
– EGE-10-13 (Directives sur les comptes et mots de passe).

---

[3] *Les institutions publiques tiennent à jour un répertoire des personnes ayant accès aux systèmes d'information contenant des données personnelles.* »

[2] De manière statistique, l'on observera que le PPDT n'a pas été sollicité, depuis le 1er janvier 2014 en tout cas, pour des directives et clauses impliquant l'exploitation de ressources informatiques et le traitement de données personnelles.

Exigences en matière de protection des données personnelles sous-traitées

Tant au sein du petit que du grand Etat, l'on retrouve de la sous-traitance de données personnelles.

Les données personnelles peuvent être confiées aux conditions de l'article 13A RIPAD[3]. L'institution demeure toutefois responsable de celles-ci, au même titre que si elle les traitait elle-même (art. 13A, al. 2 RIPAD).

S'agissant de la question de savoir si une institution publique sous-traite ou non des données personnelles et quels types de documents, le catalogue des fichiers tenu par le PPDT et contenant ces informations est public et consultable sur Internet (http://outil.ge.ch/chacatfich/#/catalog/institution). A cet égard, l'on peut mentionner le fait que tous les contrats informatiques conclus par l'Etat de Genève stipulent que le co-contractant est soumis aux obligations de la LIPAD. Enfin, en ce qui concerne les données personnelles versées aux Archives d'Etat de Genève, ces dernières ne sont pas confiées à des entreprises privées. S'il s'agit de dossiers papier, ils sont conservés dans les différents dépôts des Archives d'Etat de Genève qui sont mis à leur disposition par l'office des bâtiments et dont elles sont en principe les seules utilisatrices. S'il s'agit d'archives numériques, elles sont déposées sur la plateforme de pérennisation mise à disposition par les Archives fédérales

---

[3] L'article 13A RIPAD prévoit ce qui suit :

« *[1] Le traitement de données personnelles peut être confié à un tiers pour autant qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise.*

[2] L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même.

[3] La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant.

[4] Le recours par un sous-traitant à un autre sous-traitant (sous-traitance en cascade) n'est possible qu'avec l'accord préalable écrit de l'institution et moyennant le respect, à chaque niveau de substitution, de toutes les prescriptions du présent article.

[5] S'il implique un traitement à l'étranger, le recours à un prestataire tiers n'est possible que si la législation de l'Etat destinataire assure un niveau de protection adéquat.

[6] Le préposé cantonal publie une liste des Etats qui disposent d'une législation assurant un niveau de protection adéquat. »

(AFS) avec qui l'Etat de Genève a passé un contrat de prestations (SLA). Les AFS ne sous-traitent pas leur archivage numérique auprès d'une société privée et elles gardent la maîtrise totale de leur plateforme de pérennisation.

Pour le surplus, les entreprises privées sous-traitantes n'ont pas le droit d'utiliser les données confiées dans un autre but que celui pour lequel elles les ont reçues et ne peuvent notamment en faire commerce d'aucune manière. D'ailleurs, si elles ne sont pas soumises à la LIPAD, ces données sont soumises à la loi fédérale sur la protection des données, du 19 juin 1992 (RS LPD; 235.1) et aux principes de protection des données contenus à ses articles 4 et 5 (lesquels se retrouvent, par ailleurs, aux art. 35 et suivants LIPAD).

En effet, parmi les principes fondamentaux de protection des données, les institutions publiques sont soumises aux principes de légalité et de finalité. Il faut donc une base légale pour tout traitement de données personnelles, qui doit poursuivre un objectif conforme à la mission de l'institution publique concernée. La commercialisation de données devrait donc être prévue par une base légale pour être envisageable. Or, tel n'est pas le cas aujourd'hui à Genève.

Au bénéfice de ces explications, le Conseil d'Etat vous invite, Mesdames et Messieurs les Députés, à prendre acte de la présente réponse.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :	Le président :
Anja WYDEN GUELPA	François LONGCHAMP