REPUBLIQUE ET CANTON DE GENEVE
Préposé cantonal à la protection des données et à la transparence

Sous-traitance de données personnelles - Projet de modification du règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (RIPAD)

Avis du 22 décembre 2016

Mots clés : veille réglementaire, projet de modification, sous-traitance, données personnelles

Contexte : Par courriel du 9 décembre 2016 adressé au Préposé cantonal, M. Fabien Mangilli, Directeur de la Direction des affaires juridiques de la Chancellerie d'Etat, a soumis pour avis au Préposé cantonal à la protection des données et à la transparence un projet de 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 (RIPAD; A 2 08.01).

Bases juridiques : art. 56 al. 3 let. e LIPAD; art. 23 al. 8 RIPAD

1. Caractéristiques de la demande

Dès leur entrée en fonction, le 1er janvier 2014, les Préposés ont reçu de nombreuses sollicitations de la part des institutions soumises à la LIPAD, lesquelles souhaitent traiter les données personnelles en leur possession en dehors de leurs locaux (délocalisation) ou par le biais d'un cloud (dématérialisation).

Or, les Préposés ont dû rendre attentives ces institutions publiques au fait que cela n'était pas possible. En effet, l'art. 13 al. 6 litt. b RIPAD précise que le recours à des systèmes informatiques délocalisés ou dématérialisés permettant l'exportation sur des serveurs distants de traitements traditionnellement localisés sur des serveurs locaux ou sur le poste de l'utilisateur, notamment par la fourniture d'une plateforme technique adaptée fournie par un hébergeur tiers : a) est interdit pour toutes les données personnelles sensibles, quel que le soit le type de traitement envisagé; b) n'est possible pour les autres données que pour autant que l'intégralité du traitement survienne sur territoire suisse et que les institutions soumises au présent règlement concluent un contrat de droit public ou de droit privé tendant au traitement de données placées sous leur responsabilité.

Au demeurant, la LIPAD part de l'idée que chaque institution publique traite elle-même des données personnelles en sa possession. Elle n'envisage l'hypothèse de la sous-traitance qu'à son art. 37 al. 2, sans toutefois réglementer le sujet. Or l'expérience montre qu'en pratique, de nombreuses institutions publiques délèguent le traitement des données personnelles en leur possession, si bien qu'il apparaît nécessaire d'adapter le règlement en conséquence.

Considérant que la situation était très insatisfaisante pour les institutions publiques, les Préposés ont mis en relation la Direction générale des systèmes d'information (DGSI) avec le Groupe interdépartemental des responsables LIPAD, dans le but d'aboutir à terme à une révision adaptée du RIPAD tenant compte des besoins exprimés, dans le respect des principes de protection des données personnelles.

De la sorte, en dates des 1er et 15 septembre 2015, 27 octobre 2015, 23 mars 2016, 18 octobre 2016 et 15 novembre 2016, les Préposés ont participé aux discussions associant le Groupe interdépartemental LIPAD et la DGSI concernant la modification des dispositions de la LIPAD et du RIPAD relatives au stockage des données hors de Suisse. Ils ont attiré l'attention de ces organes sur le fait que la législation actuelle était trop contraignante par rapport au droit fédéral, lequel autorise la communication transfrontière de données, y compris à destination d'Etats n'assurant pas un niveau de protection adéquat si, par exemple, des garanties suffisantes, notamment contractuelles, permettent d'assurer un niveau de protection approprié à l'étranger (art. 6 al. 2 litt. a de la loi fédérale sur la protection des données, du 19 juin 1992; LPD; RS 235.1).

Dans son mail, M. Mangilli sollicite le préavis formel des Préposés, en vue de la constitution du dossier pour le Conseil d'Etat.

2. Modification du RIPAD

Art. 13 Sécurité des données personnelles (art. 37 de la loi) (nouvelle teneur)

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

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

Art. 13A Sous-traitance (art. 37, al. 2, de la loi) (nouveau)

[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.

Art. 14, al. 4, 2e phrase (nouvelle)

[4] […]. L'article 13A du présent règlement est applicable.

Art. 17, al. 2, lettre d (nouvelle)

Fichiers éphémères (art. 43, al. 2, de la loi)

[2] Constituent notamment des fichiers éphémères, pour autant qu'ils ne contiennent ni données sensibles ni profils de la personnalité et que leur durée de vie n'excède pas 1 an :

d) les journaux techniques qui permettent à l'institution de maîtriser ses risques en matière de sécurité de l'information.

Art. 21, al. 3 (nouvelle teneur), al. 5 (nouveau)

[3] Le responsable LIPAD collabore dans toute la mesure utile avec la direction et les organes de l'unité administrative concernée, ainsi qu'avec les responsables départementaux de la sécurité de l'information et la direction générale des systèmes d'information.

[5] Un membre de la direction générale des systèmes d'information est invité aux séances du groupe interdépartemental, mais s'abstient lors de prises de décision.

3. Appréciation

Dans la mesure où les remarques exprimées par les Préposés dans les séances susmentionnées ont été prises en compte et où l'exposé des motifs est particulièrement complet, les remarques ci-après seront succinctes.

De manière générale, les Préposés saluent le fait que le présent projet établit un cadre réglementaire clair sur la sous-traitance de données personnelles par les institutions publiques.

En préambule, les Préposés estiment que la suppression de l'obligation de tenir à jour un inventaire des subdivisions administratives des communes (art. 3 al. 3 RIPAD) fait sens, car la mise en œuvre de cette norme aurait pour conséquence d'entraîner un travail disproportionné. Au surplus, les sites Internet des communes renferment les indications nécessaires pour renseigner les citoyennes et les citoyens sur leurs subdivisions administratives.

Les Préposés jugent judicieux d'avoir fusionné en une seule disposition les questions de sous-traitance et de communication transfrontière de données (y compris le recours à des systèmes informatiques délocalisés ou dématérialisés), la communication transfrontière de données et l'informatique en nuage ne constituant finalement que des cas de sous-traitance à l'étranger.

Les Préposés considèrent important de prévoir expressément dans le contrat de sous-traitance le respect des prescriptions de la LIPAD et du règlement d'application en matière de traitement des données personnelles (art. 13A al. 3), le contrat de sous-traitance ne devant pas faire obstacle aux obligations des art. 44 ss LIPAD imposées aux institutions publiques (par exemple droit d'accès à ses données personnelles, droit de demander la rectification, la destruction ou encore d'en constater le caractère illicite, voire d'exiger la fin du traitement illicite).

L'art. 13 al. 5 du projet pose les exigences minimales en matière de sous-traitance de données personnelles (art. 13 al. 5 et 6 RIPAD en vigueur actuellement). La solution intermédiaire retenue (entre l'interdiction totale actuelle prévue par le règlement et la pratique

relativement libérale de la réglementation fédérale) convient tout à fait aux Préposés. Ces derniers comprennent que les termes de «*niveau de protection adéquat*» ont été retenus afin de suivre ceux choisis au niveau fédéral, au niveau européen, ainsi que dans le protocole additionnel à la Convention 108 (art. 6 LPD; art. 45 du règlement européen; art. 2 du protocole additionnel à la CV 108). Bien qu'ils ne se recoupent pas entièrement avec la notion plus restrictive de «niveau de *protection équivalent*» (art. 39 LIPAD), les Préposés n'y voient pas d'objection, ce d'autant plus que ces termes sont susceptibles de se recouper.

L'art. 13A al. 6 du projet met à charge l'obligation, pour le Préposé cantonal, de publier une liste des pays considérés comme assurant un niveau de protection adéquat. Avec les moyens mis à sa disposition, le Préposé cantonal n'est évidemment pas à même de se pencher sur les normes pertinentes de tous les Etats de la planète. Dès lors, il entend se fonder sur la liste établie par le Préposé fédéral pour en proposer une application par analogie.

Enfin, s'agissant de la composition du Groupe interdépartemental LIPAD (art. 21 RIPAD), les Préposés partagent l'idée selon laquelle la présence d'un membre de la DGSI aux séances de ce dernier est souhaitable, eu égard à l'éclairage technique indispensable.

* * * * * *

Le Préposé cantonal remercie la Direction des affaires juridiques de la Chancellerie d'Etat de l'avoir consulté et se tient à disposition pour tout renseignement complémentaire.

Stéphane Werly
Préposé cantonal

Pascale Byrne-Sutton
Préposée adjointe