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

# CLOUD COMPUTING

## ET PROTECTION DES DONNÉES PERSONNELLES AU SEIN DES INSTITUTIONS PUBLIQUES GENEVOISES

*FONDEMENTS JURIDIQUES ET ASPECTS PRATIQUES*

**PPDT** | PRÉPOSÉ CANTONAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE

Protection des données et transparence • Quai Ernest-Ansermet 18bis • 1205 Genève
Tél. +41 (22) 546 52 40 • Fax +41 (22) 546 52 49 • E-mail ppdt@etat.ge.ch • www.ge.ch/ppdt
Arrêts trams : 12, 18, Pont d'Arve, 15, Uni-Mail - Arrêts bus : 1, Ecole-de-Médecine, 2, 19, Musée d'Ethnographie

## 1 | PRÉAMBULE

La présente fiche a été élaborée à la suite du 3ème rendez-vous de la protection des données organisé par le Préposé cantonal à la protection des données et à la transparence le 31 mars 2015 et intitulé "*Cloud computing et risques – Quelles mesures pour protéger les données personnelles ?*". Adressé aux responsables et aux collaborateurs des administrations cantonales et communales, ainsi qu'aux institutions subventionnées intéressées, ce séminaire a permis à M. Sylvain Métille, Avocat et chargé de cours à l'Université de Lausanne, Mme Giovanna Di Marzo Serugendo, Professeure à l'Université de Genève et M. Gianfranco Moi, Directeur général adjoint de la DGSI, de rendre compte des différents aspects de la problématique. Les présentations des intervenants figurent sur le site internet du Préposé cantonal[1].

Elle a été mise à jour suite à une modification réglementaire entrée en vigueur le 15 février 2017.

Comprendre les enjeux et les risques du cloud computing et, plus largement, du transfert à l'étranger de données personnelles par les institutions publiques genevoises, est l'objectif poursuivi par cette brochure d'information. Cette dernière met en évidence quelques éléments clefs du dispositif en place à Genève applicable au domaine de la protection des données personnelles dans le champ particulier du traitement transfrontière, notamment de l'informatique en nuage. Dès l'entrée en fonction de la nouvelle autorité, des questions techniques très pointues ont, en effet, été posées sur différentes pratiques des institutions en matière de protection des données personnelles, par exemple sur l'utilisation de *Google Analytics* ou de données personnelles qui circulent sur des téléphones portables, telles que des informations relatives à la santé.

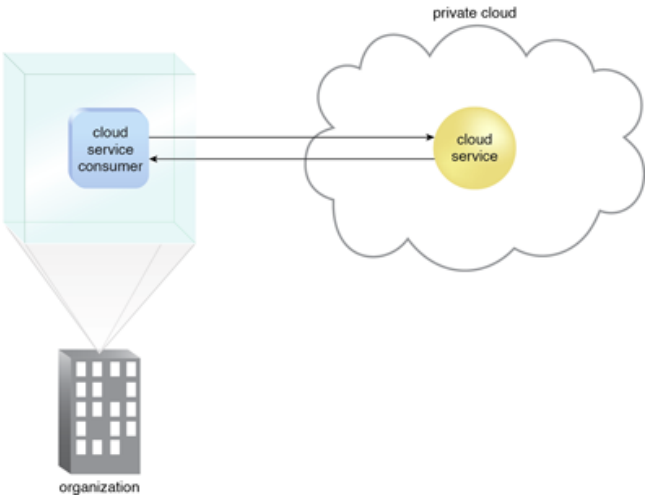
Le ***cloud computing*** (ou informatique en nuage) se définit comme l'exploitation de la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet. Les applications et les données ne se trouvent donc plus sur les réseaux internes, mais dans le nuage, et l'accès aux données, aux services et à l'infrastructure se fait à distance. L'environnement informatique (centre de calculs, espaces de stockage, logiciels de messagerie et de collaboration, environnements de développement et logiciels spéciaux tels que la gestion des relations avec la clientèle) n'est plus la propriété de l'entreprise ou de l'autorité et n'est plus géré par celle-ci, mais est loué à un ou plusieurs prestataires de services.

Il convient de distinguer :

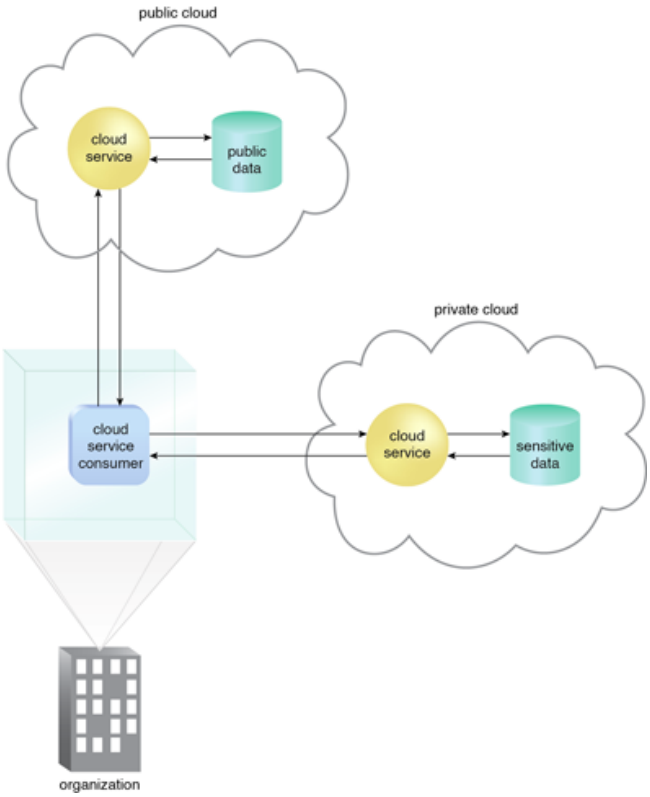
- Les nuages publics (l'infrastructure est entièrement définie et gérée par le prestataire)[2];


1 http://www.ge.ch/ppdt
2 Les illustrations qui suivent sont tirées de la présentation de Mme Giovanna Di Marzo Serugendo.

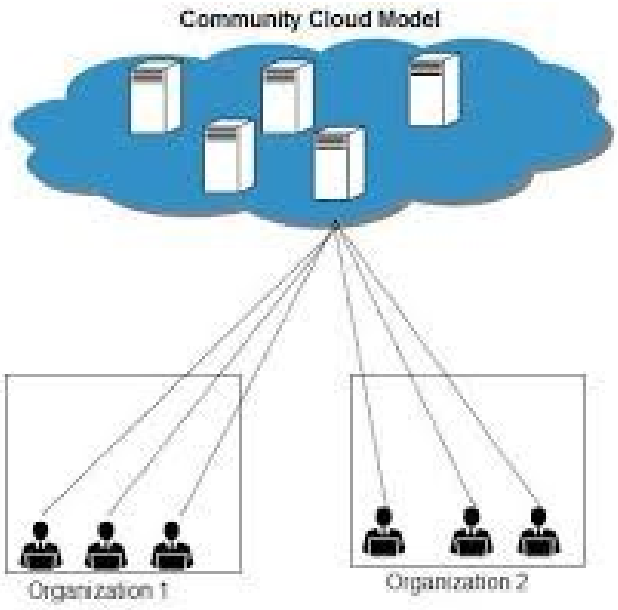
- Les nuages privés (l'entreprise elle-même ou un tiers exploite le nuage);




- Les nuages hybrides (l'entreprise utilise conjointement un nuage public et un nuage privé);



- Les nuages communautaires (plusieurs organisations utilisent la même infrastructure).




De nos jours, ***le cloud computing est omniprésent, y compris dans le secteur public***, lors de l'utilisation de *Facebook*[3], *SkyDrive*[4], *Google Drive*[5], *Dropbox*[6], *iCloud*[7], *Gmail*[8], *Google Analytics*[9], pour ne citer que quelques exemples.

La convivialité de ces services de stockage des données attire en effet de nombreuses institutions publiques. Ainsi, par exemple, les HUG externalisent des données vers le *cloud* pour leur traitement par un fournisseur externe à l'institution dans le cadre d'un logiciel de ce fournisseur selon la technique *software as a service*.

Or, le recours à l'informatique en nuage peut comporter certains risques, parmi lesquels :

- Failles au niveau de la sécurité des systèmes d'information;
- Mauvaise gestion des incidents (pannes de système et de réseau);
- Perte de contrôle sur les données, voire perte des données elles-mêmes;
- Manque de séparation et d'isolation des données;
- Non-respect des dispositions légales;
- Accès d'autorités étrangères aux données;
- Non-disponibilité des ressources et des services ou usage abusif des données[10].

Le service ***Google Analytics*** fournit aux exploitants de pages Internet des données statistiques sur les accès à leur site sans qu'il ne soit nécessaire d'installer ou d'exploiter des programmes supplémentaires du côté du serveur; il leur permet également d'analyser ces données. Pour ce faire, les exploitants doivent intégrer à leur site web un code de programme fourni par la société Google, grâce auquel cette dernière saisit les accès au site, transmet ces données aux États-Unis et les traite pour les fournir ensuite à l'exploitant. Ces opérations constituent une

---

3 Voir https://fr-fr.facebook.com/about/privacy
4 Voir http://www.microsoft.com/privacystatement/fr-ch/core/default.aspx
5 Voir https://support.google.com/docs/answer/141702?hl=fr
6 Voir https://www.dropbox.com/privacy
7 Voir http://www.apple.com/fr/privacy/
8 Voir https://www.google.com/intl/fr_ch/policies/privacy/
9 Voir https://support.google.com/analytics/answer/6004245?hl=fr
10 http://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=fr; https://secure.edps.europa.eu/EDPSWEB/edps/lang/fr/EDPS/Dataprotection/QA/QA1.

communication de données à des tiers (dans ce cas Google) dans le cadre d'une relation d'externalisation. En effet, l'adresse IP est considérée par le Préposé fédéral comme une donnée personnelle, ce que le Tribunal fédéral a confirmé[11].

# 2 | DROIT APPLICABLE

## 2.1 | Droit international

La ***Convention 108*** du Conseil de l'Europe ou Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, a été signée à Strasbourg le 28 janvier 1981[12]. Approuvée par l'Assemblée fédérale le 5 juin 1997, elle est entrée en vigueur dans notre pays le 1er février 1998[13].

S'agissant de son champ d'application, les parties signataires s'engagent à appliquer les règles fixées par la convention aux fichiers et aux traitements automatisés de données à caractère personnel tant dans les secteurs public que privé.

Cet instrument a été le premier - et reste le seul à ce jour - à prévoir des normes internationales juridiquement contraignantes spécifiquement relatives à la protection des données personnelles. Ses normes ne sont toutefois pas directement applicables (*self executing*) et les individus ne peuvent pas en tirer directement des droits.

Ce sont les parties signataires à la Convention 108 qui s'engagent à en incorporer les principes dans leur législation interne. L'objectif central de ce texte est de lutter contre les abus dans la collecte de données personnelles, de traiter des flux de données à l'extérieur des frontières nationales et de prévoir des mécanismes d'entraide et de consultation entre les parties signataires de la convention. Les principes définis par la Convention 108 touchent également à la qualité des données personnelles qui doivent être traitées de manière adéquate, pertinente, exacte et conforme au principe de la proportionnalité.

Le chapitre 3 est composé d'une seule disposition, reproduite ci-après :

*Article 12 – Flux transfrontières de données à caractère personnel et droit interne*

*1 Les dispositions suivantes s'appliquent aux transferts à travers les frontières nationales, quel que soit le support utilisé, de données à caractère personnel faisant l'objet d'un traitement automatisé ou rassemblées dans le but de les soumettre à un tel traitement.*

*2 Une Partie ne peut pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel à destination du territoire d'une autre Partie.*

*3 Toutefois, toute Partie a la faculté de déroger aux dispositions du paragraphe 2:*

*a. dans la mesure où sa législation prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel, en raison de la nature de ces données ou de ces fichiers, sauf si la réglementation de l'autre Partie apporte une protection équivalente;*

*b. lorsque le transfert est effectué à partir de son territoire vers le territoire d'un Etat non contractant par l'intermédiaire du territoire d'une autre Partie, afin d'éviter que ce tels transferts n'aboutissent à contourner la législation de la Partie visée au début du présent paragraphe.*

En matière de ***soft law***, l'organisation non gouvernementale sans but lucratif ISO (Organisation internationale de normalisation), a produit de très nombreuses normes internationales

---

11 ATF 1C_285/2009.

12 http://conventions.coe.int/treaty/fr/treaties/html/108.htm; voir le rapport explicatif du Conseil de l'Europe, http://conventions.coe.int/treaty/fr/Reports/Html/108.htm

13 RS 0.235.1

d'application volontaire. En juillet 2014 est parue la ***norme ISO/IEC 27018*** pour la protection des données personnelles dans le *cloud*, principalement destinée aux opérateurs de *cloud* agissant comme sous-traitant, ainsi qu'à leurs clients. S'inscrivant dans le prolongement des normes existantes en matière de sécurité de l'information (normes ISO 27001 et ISO 27002), cette première norme internationale spécifique à la protection des données personnelles pour le *cloud* permet aux utilisateurs de se conformer aux exigences de sécurité telles que définies par le cadre légal de protection des données personnelles. Cela par le biais d'un certain nombre de principes (consentement, transparence, communication, portabilité/destruction des données, conformité et confidentialité des données).

## *2.2 | Cadre fédéral*

***La loi fédérale sur la protection des données du 19 juin 1992***[14], complétée par l'ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993[15], s'applique aux entreprises du secteur privé ainsi qu'au secteur public relevant de la Confédération. Son champ d'application ne s'étend pas aux institutions publiques communales et cantonales genevoises. Cela dit, si la LPD n'est pas applicable aux entités publiques cantonales et communales genevoises, le droit fédéral constitue néanmoins une base de référence en matière de protection des données en tant qu'il rappelle les principes fondamentaux applicables. En outre, de nombre de questions juridiques et techniques se posent souvent de façon analogue à Genève et ont d'ores et déjà été analysées.

## *2.3 | Cadre genevois*

A Genève, ***la loi sur l'information du public, l'accès aux documents et la protection des données personnelles du 5 octobre 2001***[16] est applicable aux autorités et institutions publiques cantonales, communales et intercommunales, à leur administration, ainsi qu'aux commissions qui leur sont rattachées. Elle est complétée d'un règlement d'application du 21 décembre 2011[17], lequel permet la sous-traitance de données personnelles à certaines conditions.

# *3 | NOTIONS-CLEFS ET DEFINITIONS*

La notion de ***données personnelles*** recouvre *"toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable"* (art. 4 let. a LIPAD). Une telle identification peut être faite de multiples manières: par le biais du nom, du numéro de téléphone, de la date de naissance, de l'adresse postale, d'une adresse de courriel, d'une photo, d'un enregistrement vidéo, des empreintes digitales, de la voix, de la reconnaissance de l'iris, de l'ADN, d'un numéro d'identification personnel (numéro AVS), d'une plaque d'immatriculation automobile, etc. L'identification peut donc être directe ou indirecte.

Les données personnelles sont dites ***sensibles*** si elles portent 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 administrative (art. 4 let. b LIPAD).

Est considéré comme ***un profil de personnalité*** tout assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique, par exemple une carte de fidélité (art. 4 let. c LIPAD).

---

[14] LPD; RS 235.1
[15] OLPD; RS 235.11
[16] LIPAD; RSGE A 2 08
[17] RIPAD; RSGE A 2 08.01

Par ***traitement***, il faut entendre toute opération relative à des données personnelles - quels que soient les moyens et procédés utilisés - notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données (art. 4 let. e LIPAD).

La notion de ***maître du fichier*** (*data controller*) est inconnue de la LIPAD. Selon l'art. 3 let. i LPD, il s'agit de la personne qui décide du but et du contenu du fichier.

Le ***sous-traitant*** (data processor) est la personne qui effectue un traitement de données, sur mandat, pour le compte du maître du fichier, en respectant les instructions de ce dernier (délégation de traitement, *outsourcing*). L'utilisation de prestations dans le cadre du *cloud computing* correspond donc à un traitement de données sur mandat devant aussi bien satisfaire aux exigences du traitement des données en tant que tel qu'aux exigences de l'outsourcing dans un sens classique du terme.

## *4 PRINCIPES DE PROTECTION DES DONNEES*

Pratiquement tous les domaines de la vie des institutions publiques sont concernés par la protection des données personnelles. L'évolution des nouvelles technologies de l'information nécessite de rester constamment attentif aux règles de sécurité permettant de prévenir les risques d'atteinte à la sphère privée des personnes. A cet égard, le traitement de données personnelles doit obéir à différents principes que l'on retrouve tant dans la loi fédérale que dans la loi cantonale :

***Légalité*** (art. 35 al. 1 LIPAD). Les institutions publiques ne peuvent traiter de telles données que si l'accomplissement de leurs tâches légales le rend nécessaire. Dès lors, par exemple, si l'Université de Genève met en place un service de messagerie électronique à destination des étudiants, elle doit veiller à ce que cela entre dans ses tâches légales.

***Finalité*** (art. 35 al. 1 LIPAD). Les données personnelles ne doivent être traitées que dans le but indiqué lors de leur collecte, prévu par une loi ou qui ressort des circonstances. 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 (art. 40 al. 1 LIPAD). Par exemple, lors de la création d'un service de messagerie électronique pour les étudiants, les données personnelles suivantes peuvent être traitées par l'Université: nom, prénom, civilité et numéro d'étudiant. En revanche, au vu du principe de finalité, il ne serait pas légitime d'enregistrer le NAVS13 ou encore la catégorie socio-professionnelle des parents[18].

***Bonne foi*** (art. 38 LIPAD). Les données doivent avoir été obtenues loyalement, c'est-à-dire en toute connaissance des personnes concernées. Les données ne doivent pas être collectées à leur insu ou contre leur volonté. Ainsi, il faut que les étudiants soient en possession d'une information suffisante lors de la collecte des données : doivent être indiquées précisément les données personnelles recueillies.

***Proportionnalité*** (art. 41 al. 1 let. a LIPAD). Seules peuvent être collectées les données personnelles aptes et nécessaires à atteindre un but déterminé. Par ailleurs, le traitement ne doit pas durer plus longtemps que nécessaire. Dans l'exemple susmentionné, il serait légitime de garder les données d'un étudiant trois mois après sa dernière année académique, afin que ce dernier puisse, le cas échéant, récupérer ses données; un délai plus long paraît disproportionné.

***Exactitude*** (art. 36 LIPAD). Quiconque traite des données personnelles doit s'assurer qu'elles sont exactes (par exemple qu'elles ont été saisies correctement ou qu'il n'y a pas eu confusion). L'exactitude d'une information peut évoluer au fil des ans. Les modifications

[18] Exemple tiré de Houssay, point 2.1.

doivent donc être inscrites et datées. Lorsque des informations sont fausses, l'intéressé peut requérir la rectification des données inexactes. En conséquence, si un étudiant porte un nouveau nom après un mariage, il convient à l'Université de procéder au changement; le service auquel il peut s'adresser pour exercer ses droits d'accès et de rectification doit être connu.

***Sécurité*** (art. 37 LIPAD). Les données doivent être protégées, tant sur le plan technique que juridique, conformément aux risques présentés par la nature des données en cause, à la lumière de l'ingérence à la sphère privée des personnes concernées. Cette obligation de protection pèse sur le responsable du traitement qui a la charge d'assurer la sécurité en prenant des mesures adaptées aux risques concrets et à la nature des données. Doivent être mises en place des mesures pour éviter que les données ne soient endommagées (salle sécurisée pour héberger le serveur de messagerie, redondance matérielle, etc.), et des mesures garantissant que seules les personnes autorisées y auront accès (par exemple obligation pour les étudiants de choisir un mot de passe robuste, sensibilisation pour qu'ils ne divulguent pas leur mot de passe, gestion rigoureuse des habilitations des administrateurs système, etc.).

## 5 | *RISQUES LIES A LA DELEGATION DE TRAITEMENT ET AU TRANSFERT A L'ETRANGER*

### *5.1 | Délégation de traitement*

A Genève, ***la LIPAD ne prévoit pas le recours à un sous-traitant*** (communication *controller to processor*).

Elle n'envisage que la communication d'un maître de fichier à un autre maître de fichier (*controller to controller*).

Dans une disposition d'une relative complexité, l'art. 39, la LIPAD envisage les différentes hypothèses dans lesquelles une ***communication de données personnelles*** peut être faite ***sur demande*** :

- ***Entre deux institutions publiques genevoises soumises à la LIPAD*** sur requête de l'une d'elles (al. 1); dans cette première hypothèse, l'institution requise doit veiller à ce que les principes généraux de protection des données seront respectés, d'une part, et qu'aucune loi ou règlement ne s'oppose à une telle communication de données d'autres part;
- ***Entre une institution publique genevoise soumise à la LIPAD et un autre établissement de droit public suisse non soumis à la LIPAD ou une corporation ou un établissement de droit public étranger***, sur requête de celui-ci (al. 4-8); dans cette seconde hypothèse, l'institution requise doit veiller à ce que le traitement que l'établissement en question entend faire satisfait aux exigences légales assurant un niveau de protection adéquat de ces données et que la communication n'est pas contraire à une loi ou un règlement;
- ***Entre une institution publique genevoise et un tiers de droit privé***, sur requête de celui-ci (al. 9-12); dans ce troisième cas de figure, l'institution requise doit examiner préalablement s'il existe un *"intérêt digne de protection"* à la requête en s'assurant par ailleurs s'il n'existe pas un intérêt prépondérant des personnes directement concernés qui s'y opposerait. Le cas échéant, la détermination des personnes concernées par la demande doit être requise.

L'art. 14 al. 4 RIPAD précise que la transmission d'informations à un mandataire, à un prestataire de service lié à une institution par un contrat de droit privé ou public ou à un

représentant autorisé ne constitue pas une communication à un tiers de droit privé au sens de l'art. 39 al. 9 LIPAD.

Un nouvel art. 13A RIPAD, entré en vigueur le 15 février 2017, ***prévoit expressément le recours à un sous-traitant***. Il 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). Il vise de la sorte à assurer une meilleure sécurité des données personnelles en encadrant précisément leur sous-traitance, ce qui n'était pas le cas jusqu'à présent. Il est ainsi libellée:

***Art. 13A RIPAD***

*[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.*

Au ***niveau fédéral***, en matière de traitement de données personnelles par des tiers, l'art. 10a LPD indique :

*[1] Le traitement de données personnelles peut être confié à un tiers pour autant qu'une convention ou la loi le prévoie et que les conditions suivantes soient remplies:*
*a. seuls les traitements que le mandant serait en droit d'effectuer lui-même sont effectués;*
*b. aucune obligation légale ou contractuelle de garder le secret ne l'interdit.*

*[2] Le mandant doit en particulier s'assurer que le tiers garantit la sécurité des données.*

*[3] Le tiers peut faire valoir les mêmes motifs justificatifs que le mandant.*

## *5.2 | Transfert à l'étranger*

La communication transfrontière signifie que des données personnelles passent, par la volonté de l'auteur du traitement, de l'ordre juridique d'un Etat à celui d'un autre.

L'art. 39 al. 6 à 8 LIPAD prévoit, à certaines conditions, la possibilité de communiquer des données personnelles à une corporation ou un établissement de droit public étranger. S'il s'agit d'un tiers de droit privé domicilié hors de Suisse, les al. 9 à 12 de l'art. 39 LIPAD sont applicables.

Avant le 15 février 2017, le recours à un *cloud computing* hébergé par un tiers était permis uniquement si les données (non sensibles) et les profils de la personnalité étaient hébergés en Suisse.

La solution offerte par le ***nouvel article 13A RIPAD*** adapte le cadre réglementaire à la pratique fédérale et européenne, tout en limitant la communication de données vers des Etats assurant

un niveau de protection adéquat (al. 5 et 6). La liste de ces derniers publiée par le Préposé cantonal renvoie à celle établie par le Préposé fédéral (https://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=fr).

Au ***niveau fédéral***, l'art. 6 LPD a le libellé suivant :

*[1] Aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une législation assurant un niveau de protection adéquat.*

*[2] En dépit de l'absence d'une législation assurant un niveau de protection adéquat à l'étranger, des données personnelles peuvent être communiquées à l'étranger, à l'une des conditions suivantes uniquement:*
*a. des garanties suffisantes, notamment contractuelles, permettent d'assurer un niveau de protection adéquat à l'étranger;*
*b. la personne concernée a, en l'espèce, donné son consentement;*
*c. le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et les données traitées concernent le cocontractant;*
*d. la communication est, en l'espèce, indispensable soit à la sauvegarde d'un intérêt public prépondérant, soit à la constatation, l'exercice ou la défense d'un droit en justice;*
*e. la communication est, en l'espèce, nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée;*
*f. la personne concernée a rendu les données accessibles à tout un chacun et elle ne s'est pas opposée formellement au traitement;*
*g. la communication a lieu au sein d'une même personne morale ou société ou entre des personnes morales ou sociétés réunies sous une direction unique, dans la mesure où les parties sont soumises à des règles de protection des données qui garantissent un niveau de protection adéquat.*

*[3] Le Préposé fédéral à la protection des données et à la transparence (préposé, art. 26) doit être informé des garanties données visées à l'al. 2, let. a, et des règles de protection des données visées à l'al. 2, let. g. Le Conseil fédéral règle les modalités du devoir d'information.*

A teneur de ***l'art. 5 OLPD***, la publication de données personnelles au moyen de services d'information et de communication automatisés (Internet) afin d'informer le public n'est pas assimilée à une communication à l'étranger. Il en va autrement d'un intranet consultable depuis l'étranger ou d'un accès personnalisé à un site ouvert à certains destinataires localisés à l'étranger.

Sur la base de l'art. 6 LPD, le Préposé fédéral à la protection des données et à la transparence a établi une ***liste de pays dits sûrs***, dans lesquels la législation assure un niveau de protection adéquat. Il en va ainsi des pays membres de l'Union européenne.

En revanche, un *data center* hébergé aux Etats-Unis n'est pas sans poser problèmes pour les entreprises européennes, et notamment suisses, du fait notamment du *Patriot Act* américain, qui permet d'accéder à toute donnée hébergée par une société américaine en cas de risques liés au terrorisme.

En vertu de l'art. 25 de la Directive 95/46/CE, le transfert de données à caractère personnel vers un pays tiers à l'Union européenne est, en principe, interdit, sauf si le pays de destination assure un niveau de protection adéquat des données personnelles. La Commission européenne peut constater qu'un Etat n'appartenant pas à l'Union européenne assure un tel niveau de protection. C'est ce qu'elle a fait, pour les Etats-Unis, par une décision 2000/520/CE du 26 juillet 2000 reconnaissant les principes de la *sphère de sécurité* (*Safe Harbor*) publiés par le ministère du commerce des Etats-Unis. Dans un jugement du 6 octobre 2015 (cause C/362/14, Maximillian Schrems contre Data Protection Commissioner), la Cour de justice de l'Union européenne a cependant invalidé l'accord de protection des données conclu entre l'Europe et les Etats-Unis. En effet, selon elle, ce dernier n'offrait pas une protection suffisante en cas de transfert de données des citoyens européens sur le territoire américain. Le 8 juillet 2016, les Etats membres de l'Union européenne ont approuvé l'accord dit *Privacy Shield* (bouclier de protection de la vie privée), qui encadre désormais le transfert des données

personnelles des citoyens européens vers des centres de données (*data centers*) situés aux Etats-Unis. Le *Privacy Shield* vient changer plusieurs éléments du *Safe Harbor*, en particulier concernant l'application des principes généraux de la protection des données (information des utilisateurs, transfert à des tiers, rétention de données, etc.) et devrait normalement assurer une meilleure application de ces principes grâce aux moyens de recours et de résolutions des litiges qui seront à la disposition des utilisateurs. La Commission européenne l'a adopté formellement le 12 juillet 2016. Dans sa séance du 11 janvier 2017, le Conseil fédéral a déclaré cet accord (intitulé *Swiss-U.S. Privacy Shield*) valable et applicable au transfert de données personnelles de la Suisse à destination des Etats-Unis. L'accord suisse, qui accorde une protection équivalente à celle de l'accord *Privacy Shield* entre l'Union européenne et les Etats-Unis, prévoit la possibilité de faire appel à un ombudsman pour mener des investigations si des citoyens suisses devaient estimer que les limites fixées au gouvernement américain en matière d'accès aux données sont dépassées.

Il convient de préciser que, quelles que soient les dispositions de protection retenues, c'est le mandant qui assume la responsabilité de la protection des données: c'est à lui qu'appartient de juger des mesures qu'il estime nécessaires à la sécurité des données personnelles. Par ailleurs, si des données sont transférées à l'étranger, il doit informer les personnes quant au pays d'établissement du mandataire[19].

## *5.3 | Résumé*

En conclusion, voilà ce qu'il faut retenir au sujet du *cloud computing*, étant entendu que subsistera toujours un risque inhérent à l'utilisation de l'informatique en nuage :

- La communication transfrontière de données et l'informatique en nuage hors territoire suisse constituent des cas de sous-traitance à l'étranger.
- 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.
- 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 LIPAD et du RIPAD ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant.
- 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 de l'art. 13A RIPAD.
- 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.
- L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même.
- Dans tous les cas de sous-traitance (*processor*), il est primordial pour l'institution publique genevoise de :
    - Connaître parfaitement son cocontractant, notamment sa solidité financière, en procédant par exemple à une analyse complète des risques des points de vue organisationnel, juridique et technique;
    - Bien définir le périmètre de la tâche confiée (notamment ce qui est compris ou pas dans le prix, les limites fixées, etc.);
    - Prévoir un accord de niveau de service (*service-level agreement, SLA),* document qui définit la qualité de service requise entre un prestataire et un client;

[19] Houssay, point. 3.

- Assurer la confidentialité des données. Il faut notamment que les employés du sous-traitant s'engagent par contrat à respecter la confidentialité des données et que le prestataire n'utilise pas les données personnelles à d'autres fins (publicitaires par exemple);
- Assigner des objectifs de sécurité, les données personnelles devant être protégées contre tout traitement non autorisé par des mesures techniques et organisationnelles appropriées. Le prestataire doit protéger les données contre les risques suivants: destruction accidentelle ou non autorisée, perte accidentelle, erreurs techniques, falsification, vol ou utilisation illicite, modification, copie, accès ou autre traitement non autorisés. Ces mesures doivent faire l'objet d'un réexamen périodique sur place;
- Assurer la disponibilité et l'intégrité des données personnelles;
- Garantir la mise en œuvre des droits à la rectification et à la destruction des données traitées illicitement;
- Intégrer une clause dans le contrat permettant au client d'être tenu informé de la localisation de ses données. Un changement de lieu de traitement doit être annoncé à l'institution publique genevoise et accepté par celle-ci;
- Etre attentif au fait que le sous-traitant ne peut effectuer que les traitements que l'institution publique genevoise serait en droit d'effectuer elle-même (aucune obligation légale ou contractuelle de garder le secret ne doit l'interdire). A cet égard, le secret de fonction (par exemple l'art. 320 CP) constitue une limite au transfert de données personnelles, en ce sens qu'il impose à celui qui y est soumis de n'externaliser que dans la mesure où le secret de fonction est garanti;
- Prévoir des possibilités d'audit sur place pour contrôler ce qui est fait avec les données personnelles (vérifiabilité du processus de traitement des données et du traitement concret des données – *log files*). Les droits de contrôle des organes publics ainsi que des autorités de surveillance indépendantes (Préposé à la protection des données et à la transparence) doivent être prévus. Cela concerne aussi la possibilité de contrôles sur le site. En outre, le fournisseur de Cloud doit s'engager à procéder à des contrôles externes réguliers, d'après les standards internationaux d'audit;
- Interdire la sous-délégation sauf accord préalable écrit de l'institution;
- Empêcher que le contrat puisse être modifié unilatéralement;
- Envisager des sanctions;
- Prévoir ce qui va se passer à la fin du contrat (disponibilité, transition, restitution/destruction des données, etc.). Ainsi, dès la fin du contrat, le mandataire devra procéder à la destruction ou à la restitution intégrale de toutes les données;
- Indiquer que le contrat est soumis au droit suisse et que le for se trouve à Genève.

- S'agissant de l'usage de ***Google Analytics***, il convient en outre de :
  - Indiquer dans la page "Mentions légales" que le site de l'institution publique genevoise utilise *Google Analytics* et que cela implique l'enregistrement des adresses IP des visiteurs sur des serveurs de *Google* situés aux États-Unis;
  - Mettre en ligne une charte *Google Analytics* qui explique aux internautes le fonctionnement de cet outil d'analyse (genre et volume des données traitées) et les modalités de respect de la sphère privée de l'internaute;

- Programmer les logiciels de manière à respecter les exigences de protection des données de sorte que, par défaut, les données personnelles de l'internaute (y compris son adresse IP et les cookies) ne soient pas enregistrées, interconnectées avec d'autres données ou communiquées à des tiers et que l'analyse personnalisée de comportement et le profilage des utilisateurs ne puisse pas intervenir à l'insu de ceux-ci, sans leur consentement libre, spécifique et éclairé;
- Procéder ou faire procéder, par l'exploitant du site web, au raccourcissement des adresses IP au moyen de réglages dans le code de programmation. Dans *Google Analytics*, cela se fait en complétant le code de suivi par la fonction "_anonymizeIp()".

## *6 | LECTURES COMPLEMENTAIRES*


- ANSSI Agence nationale de la sécurité des systèmes d'information, "Maîtriser les risques de l'infogérance", décembre 2010, www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf;
- BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., "Cloud Computing - Evolution in der Technik, Revolution im Business - BITKOM-Leitfaden", octobre 2009, www.bitkom.org/de/themen/36129_61111.aspx;
- BSI Bundesamt für die Sicherheit in der Informationstechnik, "Sicherheitsempfehlungen für Cloud Computing Anbieter - Mindestsicherheitsanforderungen in der Informationssicherheit", mai 2011, https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html;
- Bundesamt für Sicherheit in der Informationstechnik (BSI), "Eckpunktepapier, Sicherheitsempfehlungen für Cloud Computing Anbieter, Mindestsicherheitsanforderungen in der Informationssicherheit", 2011;
- CSA Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", décembre 2009; https://cloudsecurityalliance.org/csaguide.pdf;
- eGovernment Suisse, "Stratégie d'informatique en nuages des autorités suisses 2012-2020", 25 octobre 2012;
- ENISA European Network and Information Security Agency, "Benefits, risks and recommendations for information security", novembre 2009, www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment;
- ENISA European Network and Information Security Agency, "Security & Resilience in Governmental Clouds", janvier 2011, www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds;
- Fraunhofer Institut, "Cloud-Computing für die öffentliche Verwaltung - ISPRAT-Studie", novembre 2010, http://www.cloud.fraunhofer.de/de/publikationen/isprat_cloud.html;
- Houssay Solenn, "Externalisation et respect de la loi «Informatique et Libertés»", https://2009.jres.org/planning_files/article/pdf/45.pdf;
- Kling Laurent, "Sérénité dans les nuages", Flash informatique 21 août 2012, p. 39 ss;
- Leinen Simon, "Cloud, une question de confiance", Flash informatique 21 août 2012, p. 36 ss;
- Mittelberger Philipp/ Binder Gabriele, "Datenschutzrechtliche Chancen und Risiken von Cloud Computing", Jus & News 2011/2, p. 163 ss;

- Neuenschwander Eric, "Cloud Computing – eine aktuelle Betrachtung, Jusletter 1er juin 2015;
- Poggi Anne-Sophie/Lefèvre Audrey, "Les offres Cloud pour entreprises et la protection des données à caractère personnel: les recommandations dont les entreprises doivent tenir compte lorsqu'elles choisissent une offre Cloud", RLDI 106/Juillet 2014, p. 44 ss;
- Schwaninger David/Lattman Stephanie S., "Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke", Jusletter 11 mars 2013.