BCCC

AVOCATS ATTORNEYS-AT-LAW

Cloud computing et risques

Quelles mesures pour protéger les données personnelles?

31 mars 2015

Sylvain Métille email: s.metille@bccc.ch Twitter: @ntdroit

Geneva
5, rue Jacques-Balmat
PO Box 5839
CH-1211 Geneva 11
Tel +41 22 704 36 00
Fax +41 22 704 36 01

Lausanne
12, avenue des Toises
PO Box 5410
CH-1002 Lausanne
Tel +41 21 318 74 00
Fax +41 21 318 74 01

www.bccc.ch

Introduction

- **Protection des données: quelques notions**
  - **Données personnelles**
  - **Traitement**
  - **Principes**
  - **Maître du fichier/sous-traitant**
- L'informatique en nuage au sens de la LPD
- La communication au sens de la LIPAD
- Les exigences de sécurité du RIPAD
- Les conséquences du traitement de données à l'étranger
- Conclusions

Données personnelles (art. 4 LIPAD)

- **Données personnelles:** toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable

- **Données sensibles**: 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; ou des poursuites ou sanctions pénales ou administratives;

- **Profil de personnalité**: assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique.

Traitement (art. 4 LIPAD)

- **Traitement**: 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

Principes

- Base légale (35 LIPAD)
  - Si l'accomplissement des tâches légales le rend nécessaire
  - Données sensibles / profils si base légale et indispensable (ou consentement)
- Proportionnalité (36 LIPAD)
  - Des données pertinentes et nécessaires
- Exactitude (36 LIPAD)
  - Des données exactes et à jour
- Reconnaissabillité (37 LIPAD)
  - La collecte de données doit être reconnaissable
- Sécurité (37 LIPAD)
  - Des données protégées contre tout traitement non autorisé.

Maître du fichier / sous-traitant

- **Notion inconnue de la LIPAD**
- **LPD:**
  - **Maître du fichier** (*data controller*): la personne qui décide du but et du contenu du fichier (art. 3 let. i LPD)
  - **Sous-traitant** (*data processor*): la personne qui effectue un traitement de données pour le compte du maître du fichier (délégation de traitement, *outsourcing*)

Transfert à l'étranger

- **Communication transfrontière**: fait pour des données personnelles de passer, par la volonté de l'auteur du traitement, de l'ordre juridique d'un Etat à celui d'un autre, pour autant que le destinataire ne soit pas déjà en possession des données.
  - Ne sont pas considérées comme communiquées à l'étranger les données qui sont simplement publiées au moyen d'un site Internet accessible ou public (art. 5 OLPD).
  - En revanche, un intranet consultable depuis l'étranger ou un accès personnalisé à un site ouvert à certains destinataires localisés à l'étranger constituent un transfert à l'étranger.

- Protection des données: quelques notions
- **L'informatique en nuage au sens de la LPD**
  - **Délégation de traitement**
  - **Transfert à l'étranger**
- La communication au sens de la LIPAD
- Les exigences de sécurité du RIPAD
- Les conséquences du traitement de données à l'étranger
- Conclusions

Délégation de traitement

- L'art. 10a LPD permet la délégation à un sous-traitant aux conditions suivantes:
  - Seuls les traitements de données que le maître du fichier serait en droit d'effectuer lui-même sont permis
  - Aucune obligation légale ou contractuelle de garder le secret ne s'y oppose
  - Le maître du fichier doit s'assurer que le sous-traitant assure la sécurité des données

Transfert à l'étranger

- Communication transfrontière de données (art. 6 LPD): des données personnelles peuvent être transmises à l'étranger dans les cas suivants:
  - Pays **sûrs** (la législation assure un niveau de protection adéquat);
    - Liste du PFPDT (données de personnes morales pas incluses)
    - U.S. – Swiss Safe Harbor
  - Des **garanties** suffisantes, notamment **contractuelles**, assurent un niveau de protection adéquat
  - **Consentement** dans le cas d'espèce
  - Le traitement est en relation directe avec la conclusion/l'exécution d'un contrat (les données traitées concernent le **cocontractant**)
  - Un **intérêt public** prépondérant, la constatation, l'exercice ou la défense d'un droit en justice
  - Données rendues **accessibles à tout un chacun** par la personne concernée (et elle ne s'est pas opposée formellement au traitement)
  - Au sein d'une même personne morale ou société ou entre des personnes morales ou sociétés réunies sous une direction unique (**règles intragroupes**).

- Protection des données: quelques notions
- L'informatique en nuage au sens de la LPD
- **La communication au sens de la LIPAD**
  - **à une autre institution soumise à la LIPAD**
  - **à une corporation ou établissement de droit public suisse**
  - **à l'étranger**
  - **à une personne de droit privé**
- Les exigences de sécurité du RIPAD
- Les conséquences du traitement de données à l'étranger
- Conclusions

Communication (art. 39 LIPAD)

- Il n'y a pas de sous-traitant dans la LIPAD (communication *controller to processor*)

- La LIPAD distingue la communication (*controller to controller*):
  - A une autre institution publique soumise à la LIPAD
  - A une corporation ou un établissement de droit public suisse non soumis à la loi
  - A une corporation ou un établissement de droit public étranger
  - A une tierce personne de droit privé

Communication à une autre institution soumise à la LIPAD (art. 39 al. 1 à 3 LIPAD)

- [1] 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 est **conforme à la LIPAD**;
  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](communication aux autorités judiciaires).

Communication à une corporation ou un établissement de droit public suisse non soumis à la loi (art. 39 al. 4 à 5 LIPAD)

- [4] La communication n'est possible que si, cumulativement:
  a) l 'entité **requérante** démontre que le traitement qu'elle entend faire des données sollicitées **satisfait à des exigences légales assurant un niveau de protection adéquat** de ces données;

  b) la communication des données considérées n'est **pas contraire à une loi ou un règlement**.
- [5] L'organe requis est tenu de s'assurer du respect des conditions posées à l'alinéa 4 et, avant de procéder à la communication requise, 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. S'il y a lieu, il assortit la communication de charges et conditions.

Communication à une corporation ou un établissement de droit public étranger (art. 39 al. 6 à 8 LIPAD)

- [6] La communication n'est possible que si, cumulativement:
  a) l'entité **requérante** démontre que le traitement qu'elle entend faire des données sollicitées **satisfait à des exigences légales assurant un niveau de protection de ces données équivalant** aux garanties offertes par la présente loi;
  b) la communication des données considérées n'est **pas contraire à une loi ou un règlement**.
- [7] En l'absence du niveau de protection des données requis par l'alinéa précédent, la communication n'est possible que si elle n'est pas contraire à une loi ou un règlement et si, alternativement :
  a) elle intervient avec le **consentement** explicite, libre et éclairé de la personne concernée ou dans son intérêt manifeste;
  b) elle est dictée par un **intérêt public important manifestement prépondérant** reconnu par l'organe requis et que l'entité requérante fournit des garanties fiables suffisantes quant au respect des droits fondamentaux de la personne concernée;
  c) le **droit fédéral** ou un traité international le **prévoit**.
- [8] L'organe requis est tenu de consulter le préposé cantonal avant toute communication. S'il y a lieu, il assortit la communication de charges ou conditions.

Communication à une tierce personne de droit privé (art. 39 al. 9 à 12 LIPAD)

- [9] La communication de données personnelles à une tierce personne de droit privé n'est possible, alternativement, que si :

  a) une **loi** ou un règlement le **prévoit explicitement**;

  b) un **intérêt** privé digne de protection **du requérant le justifie** sans qu'un intérêt prépondérant des personnes concernées ne s'y oppose.

- [10] Dans les cas visés à l'alinéa 9, lettre b, l'organe requis est tenu de consulter les personnes concernées avant toute communication, à moins que cela n'implique un travail disproportionné. A défaut d'avoir pu recueillir cette détermination, ou en cas d'opposition d'une personne consultée, l'organe requis sollicite le préavis du préposé cantonal. La communication peut être assortie de charges et conditions, notamment pour garantir un niveau de protection adéquat des données.

- [11] Outre aux parties, l'organe requis communique sa décision aux personnes consultées.

- [12] L'accès de proches aux données de personnes décédées est régi par l'article 48.

Donc (1)…

- La sous-traitance est interdite au sens de la LIPAD?

  ou

- La sous-traitance n'est pas prévue mais on applique *mutatis mutandis* les exigences de l'art. 39 LIPAD?

- Que dit le RIPAD?

Communication de données personnelles

- 14al. 4 RIPAD
  - Ne constitue pas une communication à un tiers de droit privé au sens de l'art. 39 al. 9 LIPAD 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.

- Protection des données: quelques notions
- L'informatique en nuage au sens de la LPD
- La communication au sens de la LIPAD
- **Les exigences de sécurité du RIPAD**
  - **traitement transfrontière**
  - **informatique en nuage**
- Les conséquences du traitement de données à l'étranger
- Conclusions

Sécurité des données (13 RIPAD)

- **Traitement transfrontières de données**
- [5] Les systèmes d'information et les systèmes informatiques d'une institution soumise au présent règlement permettant le traitement des **données sensibles**, des données **fiscales**, des données **relatives à des élèves ou à des mineurs**, ainsi que des données **relatives au personnel**, doivent garantir que, quelle que soit la technologie utilisée, **aucun traitement de données ne survienne hors du territoire suisse**.

Sécurité des données (13 RIPAD)

- **Systèmes informatiques délocalisés**
- [6] Le recours à des systèmes informatiques délocalisés ou dématérialisés (**informatique en nuage**) 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. Il incombe alors à l'institution de veiller au respect de toutes les prescriptions visées aux alinéas 1 à 6.

Donc (2)…

- La sous-traitance est interdite au sens de la LIPAD ou elle n'est pas prévue et on applique *mutatis mutandis* les exigences de 39 LIPAD?

- L'article 13 RIPAD introduit de nouvelles exigences… mais mentionne un cas de sous-traitance!

- Protection des données: quelques notions
- L'informatique en nuage au sens de la LPD
- La communication au sens de la LIPAD
- Les exigences de sécurité du RIPAD
- **Les conséquences du traitement de données à l'étranger**
  - **application du droit étranger**
  - **secret de fonction**
- Conclusions

Application du droit étranger

- Le droit suisse/genevois ne s'applique pas (complétement):
  - Pas de sanction à l'étranger en vertu du droit suisse en cas de violation de secrets
  - Perte du droit de refuser de témoigner ou livrer les données à l'étranger en vertu du droit suisse
- Le droit étranger s'applique:
  - Possibilités d'accès de tiers (autorités, concurrents, etc.)
  - Potentielles obligations d'annoncer des failles dans la protection des données

Microsoft fights US warrant for customer data stored overseas

Company says demand for emails stored in Ireland violates foreign sovereignty, erodes trust in US firms. US says it's essential for crime fighting.

by Edward Moyer @edatnews / June 11, 2014 3:30 PM PDT

In the latest challenge to the reach of law enforcement in the digital age, Microsoft and its Web-based email service are pushing back against a US government search warrant for customer emails stored in a data center overseas.

CBS

In court papers made public Monday, Microsoft's attorneys list their objections to a judge's order that the company comply with a warrant issued in December for a customer's email-account data stored in Dublin, Ireland.

"The government takes the extraordinary position," the filing reads, "that by merely serving such a warrant on any US-based email provider, it has the right to obtain the private emails of any subscriber, no matter where in the world the data may be located, and without the knowledge or consent of the subscriber or the relevant foreign government where the data is stored."

The release of the court papers follows a year of high-profile challenges to government access to data, which were sparked by former National Security Agency contractor Edward Snowden's leak of secret agency documents.

Among other things, the Snowden controversy raised questions about whether laws related to search and seizure need to be updated in light of rapid technological change that's made it easier to scoop up all sorts of data, including private phone calls, email exchanges, photos, and videos.

Autres limites au transfert

- Le secret de fonction (notamment 320 CP):
  - Impose à celui qui y est soumis de n'externaliser que dans la mesure où le secret de fonction est garanti
  - Cette externalisation est possible en Suisse, mais *quid* à l'étranger ?

Conclusions (1)

- **LIPAD / RIPAD**
  - **Cloud** hébergé par un tiers (y compris en Suisse) est **interdit** pour toutes les **données sensibles**.
  - Cloud hébergé par un tiers est permis seulement en Suisse pour les données autres que sensibles (permis pour les profils de personnalité).
  - Traitement de données **sensibles**, données **fiscales**, données relatives à des **élèves** ou à des **mineurs**, ainsi que données relatives au **personnel** est **interdit à l'étranger**
- **CP**
  - Attention aux données protégées par un **secret!**

Conclusion (2)

- Dans tous les cas de sous-traitance:
  - Choisir et connaître son cocontractant
  - Eviter la sous-délégation
  - Assurer la confidentialité des données
  - Assurer la sécurité
  - Bien définir le périmètre
  - Prévoir des niveaux de service (SLA), des sanctions, des possibilités d'audit
  - Pas de modification unilatérale du contrat
  - Envisager la fin du contrat (disponibilité, transition, etc.)
  - Droit suisse et for à Genève

Encore des questions?

Merci!

BCCC

AVOCATS ATTORNEYS-AT-LAW

s.metille@bccc.ch