La révision de la loi fédérale sur la protection des données

Partie 2 – cinq aspects choisis

Société genevoise de droit et de législation
8 janvier 2018

Plan

A. Devoir d'information

B. Exigences en matière de consentement

C. Communications de données personnelles à l'étranger

D. Aperçu d'autres nouvelles mesures

- Registre des activités de traitement
- Analyse d'impact relative à la protection des données personnelles *(DPIA)*
- Codes de conduite

E. Mesures concrètes à envisager pour viser la conformité aux nouvelles règles

A. Devoir d'information (1/3)

1. Modalités (article 17 P-LPD)

a) **Qui?** Obligation du responsable du traitement à l'égard de la personne concernée

- si les données personnelles sont collectées auprès de la personne concernée (collecte directe)
- si les données personnelles proviennent d'une autre source, par exemple un tiers ou une autorité (collecte indirecte)

b) **Quand?** Information doit en principe intervenir *au moment* de la collecte des données

- *Exception*: si les données personnelles ne sont pas collectées auprès de la personne concernée (mais proviennent d'une autre source), information dans un délai d'*un mois* à compter de l'obtention des données → nécessite une démarche active du responsable du traitement
- *Exception à l'exception*: si les données personnelles sont ensuite communiquées à un tiers avant le délai d'un mois, l'information doit intervenir avant la communication

c) **Comment?** Information peut être fournie par paliers: (i) information de base avec (ii) renvoi à une *privacy notice* sur un site Internet et (iii) mention de coordonnées de contact pour des questions spécifiques

d) **Sanction pénale** (CHF 250'000) en cas de violation intentionnelle du devoir d'information (omission ou fourniture d'informations inexactes ou incomplètes)

e) **Corollaire du devoir d'information**: droit d'accès aux données personnelles (articles 23 à 25 P-LPD)

A. Devoir d'information (2/3)

2. Contenu matériel du devoir d'information

Contenu minimal	• Nom et coordonnées de contact du responsable du traitement • Finalité du traitement
Contenu minimum additionnel dans certaines situations	• *Si les données personnelles sont transmises à des tiers*: destinataires ou catégories de destinataires auxquels les données personnelles sont transmises. Exemples: autorités, sous-traitants, sociétés affiliées • *Si les données personnelles ne sont pas collectées auprès de la personne concernée*: catégories de données personnelles traitées • *Si les données personnelles sont communiquées à l'étranger*: nom de l'Etat de destination et base légale si communication vers un Etat "non-adéquat" (cf. *slides* 8 ss) • *Si décision individuelle automatisée*: devoir d'information spécifique (article 19 (1) P-LPD)
Clause générale	Les informations nécessaires pour que la personne concernée puisse faire valoir ses droits selon le P-LPD et pour que la transparence soit garantie (cf. notamment la liste plus extensive prévue à l'article 13 RGPD). Exemples: • Base juridique du traitement • Durée de conservation des données (ou critères utilisés pour fixer cette durée) • Droits de la personne concernée (par exemple droit de demander l'accès / droit de retirer le consentement)

A. Devoir d'information (3/3)

3. **Exceptions au devoir d'information (article 18 (1) et (2) P-LPD)**

   a) La personne concernée dispose déjà des informations (→ importance pratique si le "collecteur initial" peut remplir les devoirs d'information des récipiendaires ultérieurs).

   b) Le traitement des données personnelles est prévu par la loi.

   c) Le responsable du traitement (personne privée) est lié par une obligation légale de maintenir le secret.

   d) Un média peut se prévaloir des dispositions en matière de protection des sources.

   e) Les données personnelles ne sont pas collectées auprès de la personne concernée (collecte indirecte) et:

      - l'information est impossible à donner; ou
      - le respect du devoir d'information implique des efforts disproportionnés.

4. **Restrictions au devoir d'information (si le responsable du traitement est une personne privée) (article 18 (3) P-LPD)** → pesée des intérêts qui peut évoluer dans le temps

   a) Information empêcherait d'atteindre le but visé par la collecte de données;

   b) Intérêt prépondérant de tiers;

   c) Intérêt prépondérant du responsable du traitement *et les données personnelles n'ont pas été communiquées à des tiers* (y compris une autorité ou une société affiliée).

B. Exigences en matière de consentement (1/2)

1. Systématique de la règlementation (en cas de traitement par des personnes privées)

a) Approche "suisse" de la protection des données

- Un traitement de données personnelles ne constitue pas *ipso facto* une atteinte à la personnalité qui requiert un motif justificatif.
  - *Exception*: La communication de *données personnelles sensibles* à des tiers requiert toujours un motif justificatif.
- Un traitement de données personnelles peut être constitutif d'une atteinte à la personnalité, par exemple:
  - en raison de son intensité (atteinte à l'"intégrité informationnelle de la personne concernée"); ou
  - en raison d'un non-respect des principes généraux en matière de protection des données.

  Dans ce cas de figure, le traitement doit faire l'objet d'un motif justificatif:

  1. Consentement
  2. Intérêt prépondérant privé ou public
  3. Base légale

b) Approche "européenne" de la protection des données

- Tout traitement de données personnelles doit nécessairement être couvert par un motif justificatif.

→ En pratique:

Le responsable du traitement cherchera à fonder tout traitement de données personnelles sur un motif justificatif, *mais* le consentement ne constitue pas le seul motif justificatif envisageable.

B. Exigences en matière de consentement (2/2)

Si le motif justificatif d'un traitement de données personnelles est le *consentement* de la personne concernée:

- **Exigences générales applicables au consentement *ordinaire* en tant que motif justificatif (article 5 (6) P-LPD)**

  Consentement doit être (i) libre, (ii) clair, (iii) précis et (iv) donné sur une base dûment informée.

  - Application du principe de proportionnalité: Plus les données sont sensibles ou plus le traitement est risqué, plus le consentement doit être clair.
  - Le consentement *ordinaire* n'est pas soumis à une exigence de forme. Le consentement *ordinaire* peut être donné tacitement (aux conditions de l'article 6 CO).
  - Le consentement peut être retiré en tout moment.

- **Exigences spéciales applicables au consentement *qualifié* en tant que motif justificatif (article 5 (6) P-LPD *in fine*)**

  a) Champ d'application: Un traitement de données sensibles ou un profilage doit être justifié par le *consentement* de la personne concernée.

  b) Consentement doit être "exprès" / "ausdrücklich" / "espresso", ce qui signifie, selon le Message (FF 2017 6647-6648), que:

  - la déclaration de volonté est formulée oralement, par écrit ou par un signe (comportement actif); et
  - la déclaration découle directement des termes employés ou du signe en question.

C. Communication de données personnelles à l'étranger (1/4)

1. Constat préliminaire: Le P-LPD n'apporte pas de changements matériels par rapport à la règlementation actuelle.

2. Distinction entre deux hypothèses:

   a) **Hypothèse 1**: L'Etat de destination dispose d'une législation assurant un niveau de protection "adéquat".

   b) **Hypothèse 2**: L'Etat de destination ne dispose pas d'une législation assurant un niveau de protection "adéquat".

3. La publications de données *online* afin d'informer le public (médias) n'équivaut pas à une communication à l'étranger, même si les données sont consultables depuis l'étranger (article 15 P-LPD).

C. Communication de données personnelles à l'étranger (2/4)

Hypothèse 1 – Communication vers un Etat "adéquat" (article 13 (1) P-LPD)

1. **Etats concernés**

   a) Tous les Etats (i) qui ont adhéré à la Convention (révisée) 108 du Conseil de l'Europe et (ii) qui la mette effectivement en œuvre

   b) La "liste du Préposé" (art. 7 OLPD actuelle) sera remplacée par une ordonnance du Conseil fédéral.

   c) En pratique: Tous les Etats Membres de l'Union européenne figureront sur cette liste.

2. **Conséquences**

   a) Le transfert de données personnelles vers ces Etats ne déclenche pas d'exigences supplémentaires.

   b) Les principes généraux en matière de protection des données (article 5 P-LPD: licéité / bonne foi / proportionnalité / finalité) doivent néanmoins être respectés.

C. Communication de données personnelles à l'étranger (3/4)

Hypothèse 2 – Communication vers un Etat "non-adéquat"

Option 2A – garanties spécifiques (article 13 (2) et (3) P-LPD)

1. **Deux options principales**

   a) *Règlement dans le contrat conclu entre celui qui communique et celui qui reçoit*: Utilisation des clauses-types de protection des données déjà reconnues par le Préposé (par exemple les "clauses contractuelles types de l'UE") (article 13 (2) (d) P-LPD)

   - Possibilité également de recourir à des clauses-types spécifiques à faire approuver par le Préposé (délai pour la prise de position: en principe 3 mois)

   b) *Au sein de groupes de sociétés*: Utilisation de *Binding Corporate Rules* (*BCR* / "contrat intra-groupe") approuvées par le Préposé ou par une autorité d'un Etat "adéquat" (article 13 (2) (e) P-LPD)

2. **Quatre autres options envisageables**

   a) Traité international (article 13 (2) (a) P-LPD)

   b) Clause contractuelle *ad hoc* incorporée dans le contrat entre celui qui communique et celui qui reçoit (article 13 (2) (b) P-LPD)

   - Clause doit être communiquée au Préposé
   - Pas d'exigence d'approbation, mais le Préposé peut ouvrir une enquête si la clause ne lui semble pas suffisante.

   c) Garanties spécifiques établies par un organe fédéral et communiquées au Préposé (article 13 (2) (c) P-LPD)

   d) Autres garanties prévues par le Conseil fédéral (article 13 (3) P-LPD) → par exemple le *Swiss-US Privacy Shield*

C. Communication de données personnelles à l'étranger (4/4)

Hypothèse 2 – Communication vers un Etat "non-adéquat"

Option 2B – 7 dérogations (article 14 P-LPD)

1. Consentement "exprès" de la personne concernée
2. Communication en lien avec la conclusion ou l'exécution d'un contrat:
   a) entre le responsable et la personne concernée
   b) dans l'intérêt de la personne concernée [nouveau]
3. Sauvegarde d'un intérêt public prépondérant
4. Constatation / exercice / défense d'un droit devant un tribunal *ou une autorité étrangère [nouveau]*
5. Protection de la vie ou de l'intégrité corporelle
6. Personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée expressément au traitement
7. Données dans un registre prévu par la loi et l'accès à ce registre est effectué de manière licite

→ En rouge: information du Préposé (sur demande de l'autorité), donc devoir accru de documentation pour le responsable du traitement afin de pouvoir répondre à d'éventuelles requêtes de l'autorité

D. Aperçu d'autres nouvelles mesures (1/3)

1. Registre des activités de traitement (article 11 P-LPD)

a) Obligation à charge de chaque responsable de traitement et de chaque sous-traitant (→ remplace l'obligation de "déclarer" certains fichiers sous l'empire de l'article 11a de la LPD actuelle)

- *Exception*: Le Conseil fédéral peut prévoir une exception pour les entreprises de moins de 50 collaborateurs et dont les traitements ne présentent qu'un risque limité.

b) Contenu (→ description générale de chaque traitement, mais pas le journal détaillé de chaque traitement effectué)

Registre du responsable de traitement	Registre du sous-traitant
1. Nom du responsable du traitement 2. Finalité du traitement 3. Description des catégories de personnes concernées • *Exemples*: employés, clients 4. Description des catégories de données personnelles traitées • *Exemples*: coordonnées de contact, données relatives à la santé 5. Catégories de destinataires auxquelles les données peuvent être communiquées • *Exemples:* maison-mère du Groupe, autorités de surveillance 6. Durée de conservation ou critères qui permettent de déterminer la durée de conservation (→ lien avec le principe de finalité) 7. Description générale des mesures de sécurité 8. Si communication à l'étranger, nom de l'Etat et garanties éventuelles mises en place	1. Nom du responsable du traitement *et du sous-traitant* 2. Catégories de traitements effectués pour le compte du responsable du traitement 3. Description générale des mesures de sécurité 4. Si communication à l'étranger, nom de l'Etat et garanties éventuelles mises en place

D. Aperçu d'autres nouvelles mesures (2/3)

2. Analyse d'impact relative à la protection des données personnelles (*Data Privacy Impact Assessment (DPIA)* / articles 20-21 P-LPD)

a) Concept: document formalisant (i) une description d'un traitement envisagé (processus / finalité / durée), (ii) une évaluation des risques engendrés par le traitement envisagé et (iii) les mesures prises pour réduire ce risque (article 20 (3) P-LPD)

b) "Questionnaire"

Q1: Est-ce que le traitement envisagé est susceptible d'entraîner un *risque élevé* pour la personnalité des personnes concernées?

Eléments de réponse:

- Critères: nature / étendue / circonstances / finalité du traitement
- Risque élevé *per se* si (i) traitement de données sensibles à grande échelle, (ii) profilage ou (iii) surveillance systématique de grandes parties du domaine public

Q2: Existe-il une exception à l'obligation de préparer un DPIA dans le cas d'espèce?

Eléments de réponse: Exception à l'obligation de préparer un DPIA si (i) traitement (exclusivement) en vertu d'une base légale, (ii) responsable du traitement bénéficie d'une certification (qui englobe le traitement envisagé) ou (iii) responsable de traitement se conforme à un code de conduite (qui remplit certaines conditions)

Q3: Est-ce que le DPIA doit être soumis pour consultation au Préposé?

Elément de réponse: Oui, si les mesures prévues dans le DPIA ne permettent pas de réduire sensiblement le risque
→ exception à l'obligation de consulter le Préposé si le DPIA a été soumis au conseiller à la protection des données du responsable du traitement (*data protection officer*).

D. Aperçu d'autres nouvelles mesures (3/3)

3. **Codes de conduite (article 10 P-LPD)**

a) Nouveau mécanisme d'autorégulation mis en place par le P-LPD

b) Modalités

- **Rédacteurs**: associations professionnelles / économiques dont les statuts prévoient la défense des intérêts de leurs membres
- **Objectif**: clarification de certaines dispositions du P-LPD, par exemple:
  - "Risque élevé" qui déclenche l'obligation de préparer une analyse d'impact relative à la protection des données personnelles (*DPIA*)
  - Modalités de mise en œuvre concrète du devoir d'information
  - Enjeux spécifiques liés à la vidéosurveillance, au *cloud computing* ou aux réseaux sociaux
- **Résultat**: prise de position (publiée) du Préposé
  - La prise de position du Préposé ne constitue pas une décision, *mais il en découle une présomption de conformité:*

    Message (FF 2017 6654): "[S]i le Préposé donne un avis favorable, il est à présumer qu'un comportement conforme au code de conduite ne fera pas l'objet de mesures administratives."

E. Mesures concrètes à envisager pour viser la conformité aux nouvelles règles

1. Acquérir le ***know how*** **interne** et définir une **gouvernance** en matière de protection des données
2. Etablir un **registre des activités de traitement** de données personnelles
3. Déterminer si certains processus de traitement de données personnelles correspondent à un "**profilage**" (nouvelle définition)
4. Revoir les ***privacy notices*** et les **déclarations de consentement** afin de s'assurer de leur validité
5. Définir un processus en vue de traitements futurs de données personnelles → **analyse d'impact relative à la protection des données personnelles (*DPIA*)**
6. Définir des processus pour traiter les **requêtes** des personnes concernées → droit d'accès ou droit à l'oubli
7. Définir un processus en cas de ***leak*** de données personnelles
8. Revoir les contrats conclus avec les **sous-traitants** et impliquant un traitement de données personnelles
9. Revoir les relations avec les **entités affiliées** qui traitent des données personnelles
10. Examiner la nécessité de désigner un "**représentant**" au sein de l'UE (RGPD)

Je vous remercie de votre attention.

Philipp Fischer

pfischer@obersonabels.com

+41 58 258 88 88