
# Nouvelle LPD – Premiers retours d'expériences dans le secteur bancaire

Webinaire du 2 novembre 2023

Centre de droit bancaire et financier

Emilie Jacot-Guillarmod

Lenz & Staehelin

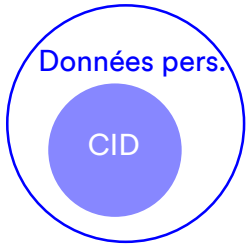
# Nouvelle LPD – Premiers retours d'expériences dans le secteur bancaire

| | | | |
|---|---|---|---|
| Fin de la protection LPD des personnes morales | Interactions entre la LPD et la Circulaire FINMA 2023/1 (risques opérationnels) | Communication suite à une fuite de données | Gestion des demandes LPD |
| Implications contractuelles (sous-traitance) | Cyber-sécurité & Registres | Envers les clients et les tiers | Des clients ou de tiers |

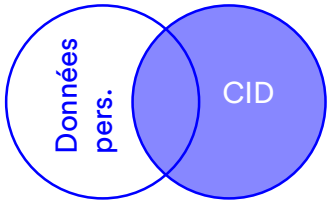
# Fin de la protection LPD des personnes morales

## Implications contractuelles (sous-traitance)

aLPD




nLPD




### *Data processing addendum* (DPA): 28 RGPD

- Traitement selon instructions documentées
- Engagement confidentialité collaborateurs
- Sous-traitance de 2ème rang: Accord préalable
- Audit
- Assistance au RT dans le respect de ses propres obligations
- Mesures de sécurité

\+ Transferts internationaux

### Secret bancaire

**Déjà nécessaire sous l'aLPD**

- Reconnaissance de la qualité de mandataire 47 LB
- Év. Background checks
- Transferts internationaux (Suisse uniquement sauf waiver)

\+ "Clauses outsourcing" (Audit, sous traitance)

**Points supplémentaires vu la nLPD**

➔ Application par analogie du DPA/assimilation des CIDs aux données personnelles?

➔ Protection "au moins aussi stricte" que données personnelles?

➔ Clause secret bancaire "renforcée"?

# Interactions entre la LPD et la Circulaire FINMA 2023/1

## Cyber-sécurité & Registres

| | nLPD | Circ. 2023/1 |
|---|---|---|
| Cybersécurité | • But: **Protection de la personnalité** des *data subjects*<br>• Mesures techniques et organisationnelles (**TOMs**) appropriées<br>• "Concrétisation" OPDo:<br>– TOMs doivent garantir la **confidentialité, disponibilité, intégrité, traçabilité**<br>– **Proportionnalité** (approche basée sur les risques, coûts/bénéfices)<br>– **Axes contrôle**: p. ex. accès, utilisation, support, transport, détection violation, restauration<br>– Dans certains cas: **journalisation** | • But: gestion des **risques opérationnels** (dommages et conséquences règlementaires pour la banque)<br>• **Gouvernance** (responsabilités, *reporting*) et documentation<br>• Identification, évaluation des risques, définition de la tolérance<br>• **Gestion** des risques<br>– TIC (y.c. change management, exploitation, incidents)<br>– Cyberrisques (actes malveillants internes/externes)<br>– Données critiques<br>– *Business continuity management* |
| Registres | • Registre des activés de traitement ("**ROPA**")<br>• **Aperçu** de toutes les traitements de données personnelles (not. finalité, catégories de données, catégories de destinataires, transferts internationaux, TOMs)<br>• **Outil de la conformité** au quotidien<br>• Accessible depuis la Suisse et à la disposition du PFPDT | • Inventaire des risques opérationnels<br>• 1 ou plusieurs inventaire(s) des **composantes TIC**<br>– *Hardware* et *software* nécessaire aux fonctions et processus critiques<br>– **Lieu de sauvegarde** des données critiques<br>– En tenant compte des interfaces avec prestataires importants |

Inventaire fonctions externalisées (Circ. 2018/3)

# Communication suite à une fuite de données

## Envers les clients et les tiers

### Violation sécurité des données

- Perte/modification/Effacement **accidentel ou illicite**
- Cause interne (collaborateurs) ou externe (prestataires, pirates)
- P. ex. cyberattaque, mais aussi support données perdu, e-mail envoyé au mauvais destinataire etc..

### Notification

- Au **PFPDT**: ASAP si risque élevé pour les pers. concernées
- À la **FINMA** (29 LFINMA + Circ. 2023/1 + Comm. 5/2020)
  - Dans les 24H puis 72H si cyberattaque importante
  - ASAP incidents TIC importants / atteinte données critiques
- Aux **pers. concernées**: ASAP si nécessaire pour leur protection
- À l'avenir: au **Centre national pour la cybersécurité** (74b LSI)

### Mesures ultérieures

- *Root cause analysis*
- **Remédiation**/ Amélioration mesures techniques et organisationnelles
- **Registre** des violations de la sécurité des données (à conserver pendant 2 ans)
- Reporting **FINMA** (29 LFINMA+ Circ. 2023/1)
-

Obligations continues: Gestion des risques TIC (Circ. 2023/1) / Mesures techniques et organisationnelles (LPD)

# Communication suite à une fuite de données

## Envers les clients et les tiers

| Violation sécurité des données | Notification | Mesures ultérieures |
|---|---|---|
| • Perte/modification/Effacement **accidentel ou illicite**<br>• Cause interne (collaborateurs) ou externe (prestataires, pirates)<br>• P. ex. cyberattaque, mais aussi support données perdu, e-mail envoyé au mauvais destinataire etc.. | • Au **PFPDT**: ASAP si risque élevé pour les pers. concernées<br>• À la **FINMA** (29 LFINMA + Circ. 2023/1 + Comm. 5/2020)<br>– Dans les 24H puis 72H si cyberattaque importante<br>– ASAP incidents TIC importants / atteinte données critiques<br>• Aux **pers. concernées**: ASAP si nécessaire pour leur protection<br>• À l'avenir: au **Centre national pour la cybersécurité** (74b LSI) | • *Root cause analysis*<br>• **Remédiation**/ Amélioration mesures techniques et organisationnelles<br>• **Registre** des violations de la sécurité des données (à conserver pendant 2 ans)<br>• Reporting **FINMA** (29 LFINMA+ Circ. 2023/1)<br>• |

Pas de communication
lorsque le secret bancaire s'y oppose
(p. ex. ADE)

# Gestion des demandes LPD

## Des clients ou de tiers

### Droit d'accès

- Titulaire: toute personne dont les données sont traitées (employé, client, tiers)
- Opposabilité : responsable du traitement
- Délai de réponse: en principe 30 jours.
- Périmètre : les données personnelle de la personne (mais non celles de tiers) + informations nécessaires à l'exercice des droits de la personne (liste selon 25 § 2 LPD).
- Format: aperçu généralement écrit des principaux aspects du traitement + copie écrite des données (consultation sur place ou information orale ne suffisent en principe pas si pers. concernée demande réponse écrite)

### Mesures organisationnelles

- **Canal de communication** (par exemple, adresse électronique dédiée)
- **Procédures internes** (responsabilités, calendrier, réponses-types)
- **Informatique** : capacité d'organiser, d'extraire et d'expurger les données

### Limites

- **Secret bancaire** (pas de réponses aux demandes de tiers si le secret bancaire s'y oppose)
- **Intérêts prépondérants?** (p. ex. AML/KYC)
- Pas communications LBA au MROS et autres autorités (34 LBA)
- Demande est manifestement infondée (***fishing expeditions***)

# Contact

## Emilie Jacot-Guillarmod

Senior Associate
MBA, INSEAD
+41 58 450 70 00
Emilie.Jacot-Guillarmod@lenzstaehelin.com
LinkedIn: https://ch.linkedin.com/in/emilie-jacot-guillarmod

Lenz & Staehelin
www.lenzstaehelin.com