Wébinaire Partie 2

Les nouvelles obligations en détail

Anna Kuhn, avocate MLaw

Esther Zysset, avocate, Docteure en droit

Programme

Partie 2: Les nouvelles obligations en détail

1 Ce qui a précédé

2 Les nouvelles obligations en détail

3 Surveillance et sanctions

4 Pro memoria: conseils pratiques pour la mise en œuvre

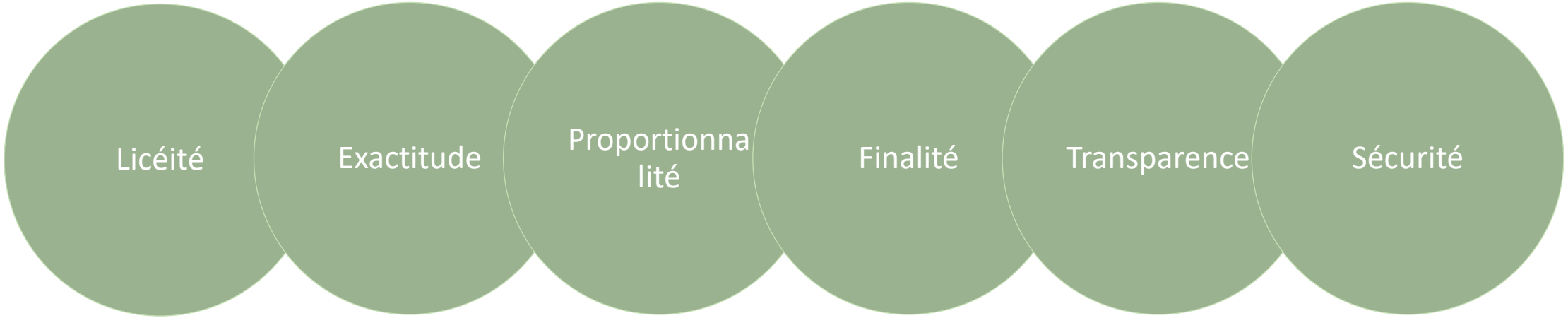
1 Ce qui a précédé 1/2

Les bases :

- Les «données personnelles» sont des données qui se rapportent à une personne identifiable ou identifiée (notion très large)
- Il existe en outre des «données personnelles sensibles»
- Toute utilisation de données personnelles représente un «traitement de données » au sens de la loi

1 Ce qui a précédé 2/2

Principes fondamentaux:



2 Les nouvelles obligations en détail

Il y en a quelques unes. . .

a) Registre des activités de traitement

b) Sous-traitance

c) Communication des données à l'étranger 🇺🇸 🇩🇪

d) Devoir d’informer

e) Devoir d’annonce des violations de la sécurité des données (*data breach notifications*)

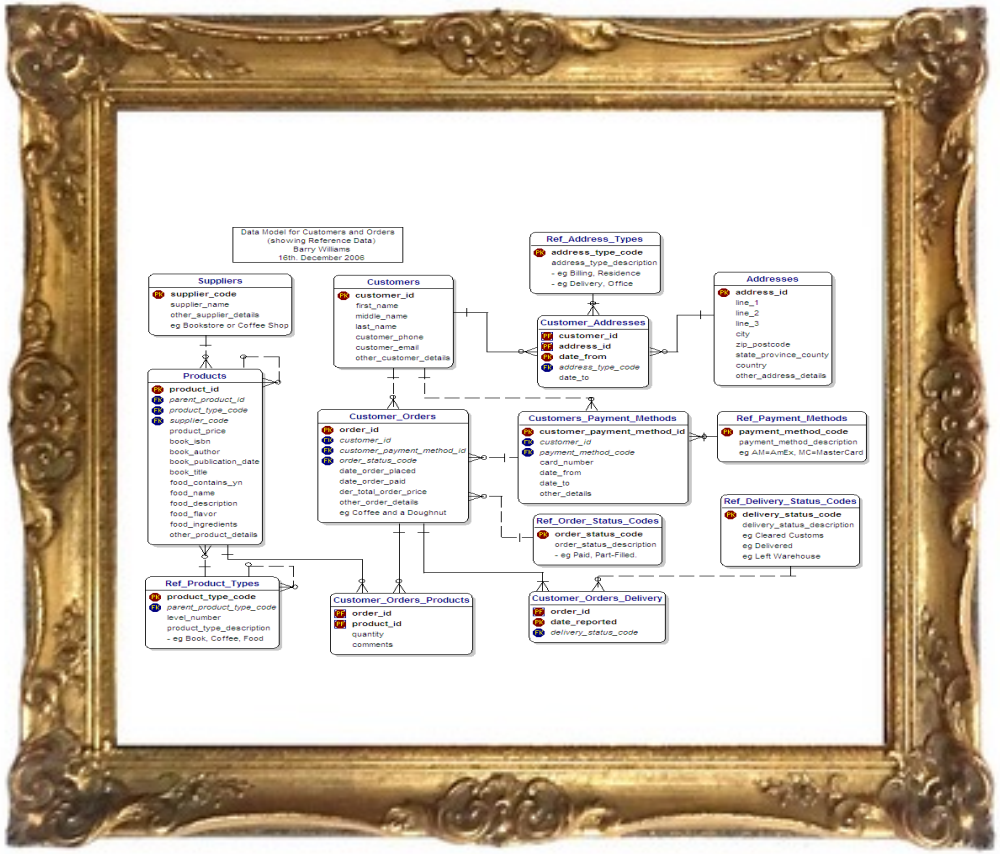
f) Analyse d’impact relative à la protection des données

g) Droits des personnes concernées

h) Conseillère interne à la protection des données

a) Registre des activités de traitement

Du chaos à la structure!



a) Registre des activités de traitement

Il s'agit d'un registre des activités relatives aux données personnelles, soit une liste contenant les **traitements de données les plus importants** (art. 12 nLPD)

La loi en fixe le **contenu minimal**:

- Identité du responsable
- Finalité du traitement
- Catégories des personnes concernées et des données personnelles traitées
- Catégories des destinataires
- Etats concernés 🇺🇸 🇩🇪 🏴‍☠️
  en cas de communication de données personnelles à l'étranger et
- Mesures de protection

a) Registre des activités de traitement

Exceptions (art. 24 OPDo):

- Entreprises qui emploient moins de 250 collaborateurs
- Personnes physiques
- Dans la mesure où leurs traitements de données impliquent un **faible risque d'atteinte** à la personnalité des personnes concernées

  → L'exception tombe en cas de traitement de données sensibles à grande échelle ou lorsque le traitement constitue un profilage à risque élevé

Les organes fédéraux déclarent leur registre d'activités de traitement **au PFPDT** (art. 12 al. 4 nLPD)

a) Registre des activités de traitement

Traitement de données pouvant entrer en ligne de compte :

- Procédures de recrutement
- Gestion des collaborateurs
- Marketing
- Finance et comptabilité, etc.

Conseils pratiques

- Orientation vers des **processus d'entreprise existants**!
- Mise en œuvre avec des tableaux Excel ou un **logiciel spécialisé de protection des données**

b) Sous-traitance

Distinction entre deux rôles

Responsable

- «Cheffe» du traitement de données
- Peut faire appel à des tiers
- Doit convenir avec eux d'une réglementation écrite relative à la sous-traitance
- Art. 5 lit. j nLPD

Sous-traitante 1

Sous-traitante 2

- Doivent se conformer aux instructions des responsables (selon réglementation écrite)
- Doivent veiller eux-mêmes à la sécurité nécessaire des données dont ils ont la charge
- Art. 5 lit. k nLPD

b) Sous-traitance

Externalisation du traitement de données

- Recours à des logiciels (z.B. CRM, Collaboration [Microsoft Teams], SAP)
- Services d'hébergement *(hosting)* par des tiers (p.ex. Site web sur AWS)
- Envoi de newsletter, services de marketing par l'intermédiaire d'une agence

La condition préalable est toujours que les tiers **traitent des données personnelles** en rapport avec la tâche qui leur est confiée.

Le sous-traitant ne peut traiter les données que **sur instruction** (art. 9 nLPD).

b) Sous-traitance

Obligation de conclure un contrat écrit (contrat de sous-traitance, *data processing agreement, DPA***)**

- Description du projet/de la prestation de service
- Indication de la finalité du traitement et interdiction d'utiliser les données à des fins personnelles (lié à la finalité)
- Obligation de ne traiter les données que sur instruction de la personne responsable
- Obligation d'indiquer les sous-traitants et les sites de données ainsi que l'obligation de faire autoriser le recours à de nouveaux sous-traitants
- Obligation de mettre en œuvre des TOMs (*technical and organisational measures*) appropriées à la sécurité des données
- Droits d'audit et obligations à la fin du contrat

c) Communication de données à l'étranger

Idée centrale = assurer une
protection adéquate des données malgré l'applicabilité d'une législation étrangère (cf. art. 16 s. nLPD)

Définition du transfert de données à l'étranger:

- Transfert à un responsable étranger (p. ex. autorité étrangère de sécurité sociale)
- Transfert à un sous-traitant étranger (p. ex. utilisation de Teams de Microsoft, USA)
- Accès à des données depuis l'étranger

Le transfert physique de données ainsi que l'**accès à distance** (*remote access*)
sont couverts.

c) Communication de données à l'étranger

Cascade pour établir un niveau de protection des données approprié

Etats tiers «sûrs»

Mesures de protection appropriées

Exceptions

Etats de l'EEE, Andorre, Norvège, Nouvelle-Zélande, etc.

États-Unis, Chine, Russie, etc.

Cf. liste de tous les États tiers à l'annexe 1 de l'OPDo

Contrat de droit international public
Clauses de protection des données (soumises au PFPDT)
Clauses standard de protection des données (p. ex. de la Commission européenne)
Binding Corporate Rules etc. + mesures supplémentaires si besoin

Consentement explicite
Sauvegarde d'intérêts publics prépondérants
Données rendues accessibles à tous
Données provenant d'un registre prévu par la loi, etc.

d) Devoir d’informer

Devoir d'**informer toutes les personnes concernées** de toute collecte de données (art. 19 ss nLPD)

Contenu minimal défini par la loi

- Identité et contact du responsable
- Finalité(s) du traitement
- Destinataires des données
- États destinataires et mesures de protection prises

d) Devoir d’informer

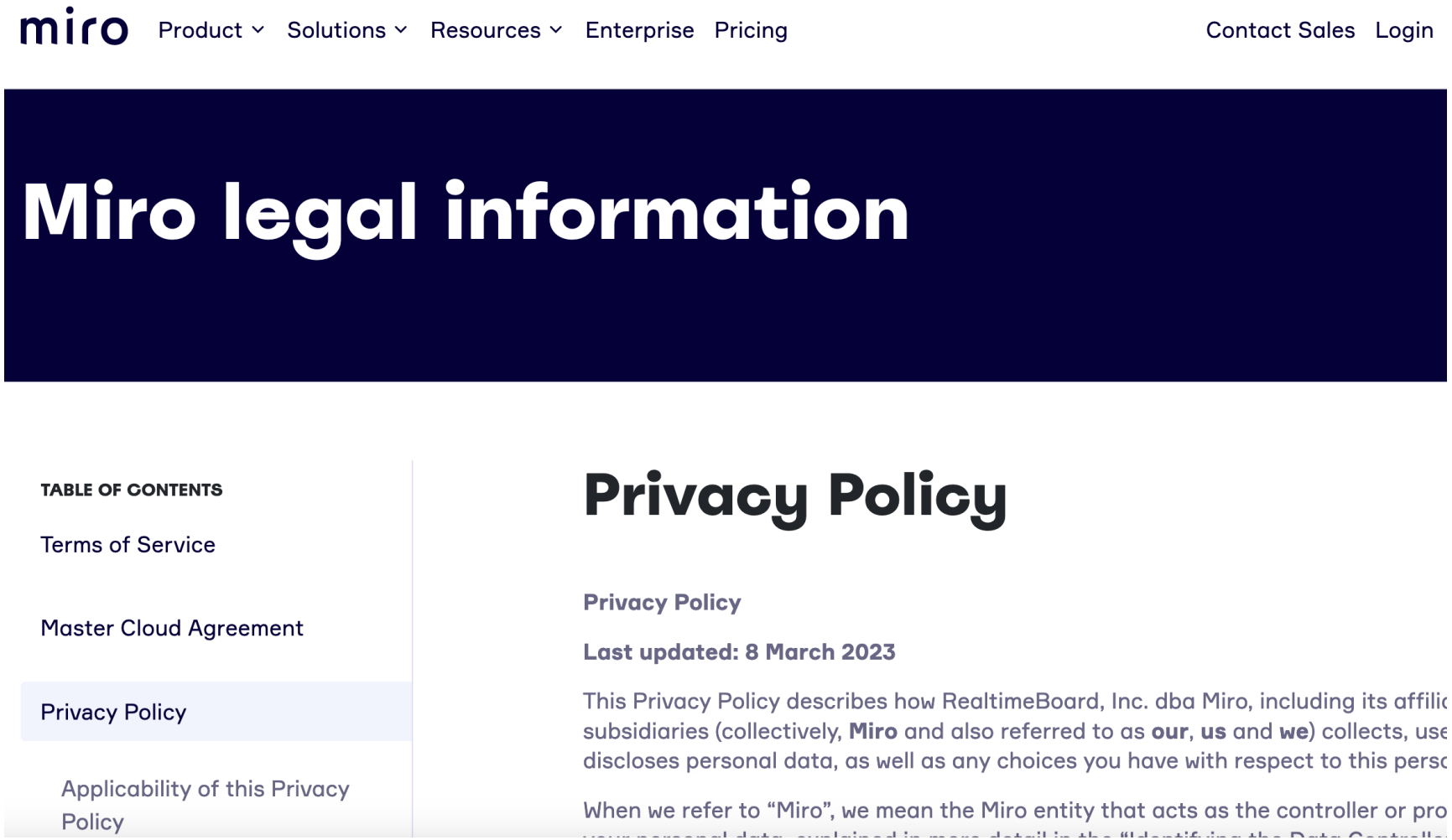
En principe, pas de prescription de forme ; **documentation et forme écrite** toutefois recommandées (pour des raisons de preuve !)

- p.ex. déclaration de protection des données du site web
- *Privacy Policy* pour les clients
- Réglement de travail pour les collaborateurs

Exigences en matière d'information (art. 13 OPDo)

- Langage précis, transparent et facile à comprendre
- Complet
- Facilement accessible

d) Devoir d’informer



e) Data Breach Notifications

Devoir d'annoncer des violations de la sécurité des données (art. 24 nLPD)

Définition (art. 5 lit. h nLPD)

- Les données personnelles sont **perdues**, **modifiées**, **effacées ou détruites**, **di vulguées** ou r**endues accessibles** à des personnes non autorisées

Exemples

- Perte d'une clé USB, d'un ordinateur ou d'un téléphone portable avec des do nnées commerciales
- Une personne non autorisée a accès aux données (p. ex. les logins ont été partagés)
- Stockage de données sur Cloud non autorisé
- Suspicion de cyberattaque (DDoS, ransomware, phishing, etc.)

e) Data Breach Notifications

Quand doit-on l'annoncer?

- Uniquement dans la mesure où la violation de la protection des données est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

A qui doit-on l'annoncer?

- A l'autorité de surveillance de la protection des données (p. ex. le PFPDT)
- Le sous-traitant signale une violation au responsable du traitement.
- A la personne concernée, si nécessaire pour sa protection (p. ex. changement de mot de passe)

e) Data Breach Notifications

Comment doit-on l'annoncer?

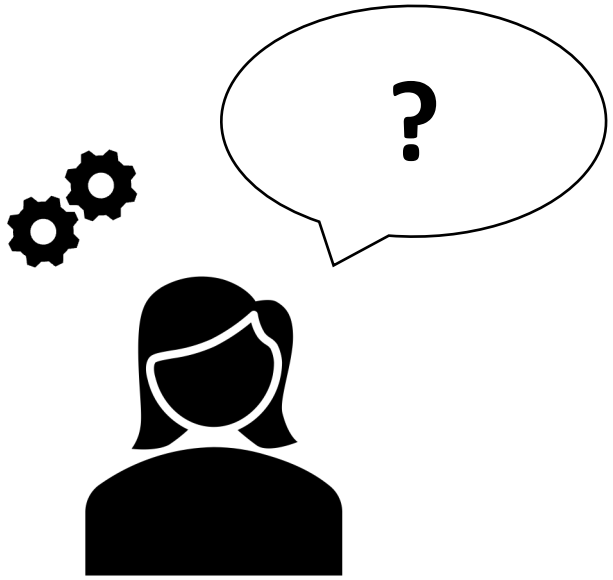
- «Dans les meilleurs délais» (art. 24 al. 3 nLPD; 72 heures selon la pratique)
- Par écrit et conservation de la documentation pendant 2 ans (art. 15 al. 4 OPDo)

Que doit-on annoncer au minimum? (art. 15 al. 1 OPDo)

- Nature de la violation
- Moment et durée
- Catégories et nombre approximatif de personnes et données personnelles concernées
- Conséquences et risques éventuels pour les personnes concernées
- Mesures prises ou prévues
- Nom et coordonnées d'une personne de contact

f) Analyse d'impact relative à la protection des données personnelles

L'analyse d'impact relative à la protection des données personnelles est une **«réflexion» documentée** sur le traitement des données (art. 22 nLPD)



f) Analyse d'impact

But: Identification et évaluation des risques liés à la protection des données (risque = dommage x probabilité de survenance)

Obligation de réalisation:

- Le/la responsable
- Avant un nouveau traitement de données personnelles ou en cas de modification importante du mode de traitement actuel; en outre, vérification périodique

Contenu:

Description	Analyse des risques	Identification des facteurs de risques particuliers	Évaluation des risques	Mesures pour maîtriser les risques	Décision relative à la présentation ou non à l'autorité de surveillance

f) Analyse d'impact

Exceptions:
- Personnes privées traitant des données en vertu d'une obligation légale
- Utilisation d'un produit / système certifié
- Respect d'un code de conduite

Marche à suivre

Risque élevé pour les droits fondamentaux?

Type, étendue, circonstances et finalité du traitement des données

Exemples:
- Traitement à grande échelle de données personnelles sensibles
- Profilage
- Surveillance systématique du domaine public

Réalisation de l'AIPD

1. Description des traitements des données
2. Evaluation des risques
3. Mesures pour réduire les risques

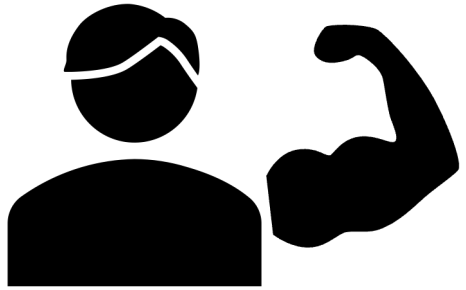
Consultation surveillance de la protection des données / personnes concernées

Lorsque malgré les mesures prises, le traitement présente encore un risque élevé pour les personnes concernées

g) Droits des personnes concernées

Les personnes concernées ont certains droits en rapport avec le traitement de leurs propres données personnelles (en particulier art. 25 ss nLPD)

Cela inclut les droits suivants:



- Droit d’accès
- Droit à l’effacement
- Droit à la rectification des données
- Droit à la remise ou à la transmission de données personnelles (en cas de traitement automatisé basé sur le consentement ou en lien avec un contrat)

g) Droits des personnes concernées

Qu’en est-il des droits des personnes concernées en général?

- Délai de 30 jours
- Identification de la personne qui fait la demande
- Demande écrite et réponse recommandées (à des fins de preuve !)
- Les droits des personnes concernées sont en principe accordés gratuitement
- Diverses exceptions doivent être prises en compte (p. ex obligations de conservation)
- Conseil pratique :la mise en œuvre dans les délais nécessite une bonne vue d'ensemble des traitements de données. Il est recommandé de mettre en place un processus si les demandes sont fréquentes.

h) Conseillère interne à la protection des données

- **Fonction de conseil** en matière de protection des données, il s'agit de la **personne de contact** pour les autorités et les personnes concernées

- Facultative pour les responsables privés traitant des données
- Obligatoire pour les organes fédéraux (possibilité de nommer conjointement)

h) Conseillère interne à la protection des données

Exigences légales quant au rôle (art. 23 s. , art. 25 ss OPDo)

- Accès aux informations nécessaires
- Dispose des ressources nécessaires
- A des connaissances spécialisées suffisantes
- Indépendance
  - …par rapport aux responsable du traitement
  - …absence de conflits d'intérêts

3 Surveillance et sanctions

Surveillance

Pouvoir d'enquête du PFPDT (art. 49 nLPD)

Le PFPDT peut, entre autres (art. 50 nLPD):

- Ordonner **l'accès** à tous les documents, locaux et installations
- Auditionner des **témoins**

Pouvoir de décision du PFPDT (art. 51 nLPD):

- Interdiction
- Adaptations
- Suppressions
- Réaliser des AIPD

3 Surveillance et sanctions

Sanctions

- Amendes jusqu'à CHF 250'000.00
- Sanctions pour les **collaborateurs** (entreprises seulement à titre exceptionnel, art. 64 al. 2 nLPD)!
- **Le dol (éventuel)** est une condition préalable

Sont notamment sanctionnés:

- Violation du devoir d'informer, d'accorder l'accès, et de collaborer (art. 60 nLPD)
- Communication de données dans un **pays tiers «non sûr» sans mesure de protections suffisantes**
- Transfert du traitement des données à des **tiers** sans assurer la sécurité des données
- Non-respect des exigences en matière de **sécurité des données**
- Insoumission à des **directives** du PFPDT (art. 63 nLPD).

4 Pro memoria: Conseils pratiques pour la mise en oeuvre

- Etape 1 – Examen des dispositions applicables
- Etape 2 - Data mapping / Registre des activités de traitement
- Etape 3 – Catalogue des mesures
- Etape 4 – Mise en oeuvre étape par étape
- Etape 5 – Revue et amélioration

Merci de votre attention.

Av. MLaw Anna Kuhn, CIPP/E
kuhn@publicsector.ch
+41 44 586 22 73

Av. Dr. iur. Esther Zysset, CIPP/E
zysset@publicsector.ch
+41 44 586 22 02

PUBLIC SECTOR LAW