nLPD – Ce qu'il faut faire.

Pour les PME

Mis en oeuvre : ☑
Nouveau dès 1.9.2023

7 Dix commandements pour le traitement des données selon la LPD[1]

1. Nous **disons** aux personnes ce que nous faisons de leurs données et pourquoi.
2. Nous **nous y tenons** et n'utilisons pas les données à d'autres fins.
3. Nous pratiquons la **minimisation des données** et le "besoin de savoir".
4. Nous **supprimons** les données dès que nous n'en avons plus besoin.
5. Nous permettons aux personnes de dire "**non**" au traitement.
6. Nous ne faisons que ce que nous trouverions **acceptable** pour nous-mêmes.
7. Nous vérifions que nos données ne contiennent pas **d'erreurs** ou de lacunes problématiques.
8. Nous ne transmettons pas de **données sensibles**[2] à des tiers.
9. Nous prenons des mesures pour garantir la **sécurité** des données chez nous.
10. Nous obtenons des données **légalement** et à partir de sources légales.

Exceptions (uniquement) possibles en cas d'intérêts légitimes prépondérants. Nous concevons chaque traitement selon ces principes !

2 Politique de confidentialité

Toute collecte planifiée de données qui n'est pas exigée par la loi doit être mentionnée dans la pol. de confidentialité.

Nous renvoyons les personnes à la politique (dans les CG, les apps, les formulaires, etc.). Elle se trouve sur notre site.

Contenu obligatoire : Qui nous sommes (avec les coordonnées), les données collectées et les finalités, les destinataires des données (noms non requis) et les pays ou régions concernés (y.c. les bases juridiques invoquées[3]).

1 Registre des traitements

Nous tenons un registre de nos traitements de données (p. ex. gestion des données clients, comptabilité, gestion RH, boutique en ligne). Son contenu est conforme à l'art. 12 nLPD, e.a. les finalités du traitement, les catégories de personnes, de données et de destinataires et la période de conservation.[4] Cette **obligation ne s'applique que** si nous avons 250+ employés (effectif) ou si nous traitons des données sensibles à grande échelle ou si nous pratiquons le profilage à risque élevé.

3 Sous-traitants sous contrôle

Si nous confions le traitement de nos données à un prestataire IT ou à une autre personne, nous concluons un "DPA", c.-à-d. un **contrat** qui nous permet de gérer et contrôler l'entreprise et d'approuver (ou de s'opposer) au préalable au recours à des tiers. Il définit aussi les **mesures de sécurité** ("TOMS"). Nous les vérifions (y.c., si nécessaire, les rapports d'audit). Un DPA selon l'art. 28 RGPD est suffisant s'il renvoie aussi à la LPD. Le sous-traitant ne peut faire que ce que nous sommes autorisés à faire (p. ex. généralement pas de traitement à des fins propres). Nous vérifions la conformité des DPA actuels/nouveaux.

5 Lorsque les données vont à l'étranger

Sans problème : EEE, UK, pays adéquats[5]

Tous les **autres pays** autorisés si e.a. :

- Transfert nécessaire à l'exécution d'un contrat avec ou dans l'intérêt de la personne concernée
- Renonciation explicite à la protection à l'étranger
- Conclusion des "clauses contractuelles types" de l'UE[6] avec adaptation CH et aucune raison de penser que l'accès aux données par des autorités sera problématique (effectuer un TIA[6,7]).

Nous vérifions nos contrats à cet égard !

4 Les données sont sécurisées, sinon nous le signalons

Mesures techniques : Accès uniquement selon le principe du "besoin de savoir" et avec un compte personnel, authentification multifacteur en cas d'accès externe, pistes d'audit (év. obligatoires pour les données sensibles[2], à conserver pendant 1 an), pseudonymisation, pare-feu, logiciel anti-malware, sauvegardes (également hors ligne).

Mesures organisationnelles : Directives (p. ex utiliser cette page), formations, examen des "logs", s'il y a beaucoup de données sensibles[2], vérifier vos mesures et créer une politique de traitement.

Devoir d'annonce : Si la confidentialité, l'intégrité ou la disponibilité des données personnelles est violée *et* qu'il existe un risque élevé de conséquences négatives pour les personnes concernées (pas simplement une nuisance), le cas doit être annoncé au PFPDT (formulaire sur https://edoeb.admin.ch) et être documenté pendant 2 ans ; si les personnes concernées ne peuvent pas se protéger elles-mêmes des conséquences, le cas doit aussi leur être annoncé.

Chacun est coresponsable de la sécurité !

6 Nous garantissons les droits des personnes concernées

Nous **identifions** correctement la personne au préalable.

Nous fournissons à une personne **ses propres données personnelles** (pas de documents) et, sur demande, certaines autres informations (en général gratuitement dans un délai de 30 jours). Nous évitons de donner l'impression que nous avons fourni toutes les données (car les renseignements faux ou incomplets sont punissables). Notre première réponse peut se limiter aux données habituellement recherchées par les personnes. La personne doit nous aider à identifier d'autres données. Les demandes non motivées par la protection des données ne sont pas protégées. Nous protégeons les données des tiers et nos propres secrets d'affaires.

Toute personne peut demander la **rectification** de ses données. Si l'exactitude est contestée, nous le signalons.

Toute personne peut demander la **suppression** de ses données ou nous demander d'arrêter ou de modifier notre traitement. Nous pouvons continuer si nous avons une raison prépondérante de le faire.

Si un **ordinateur** prend des décisions discrétionnaires ayant d'importantes conséquences négatives, nous en informons les personnes concernées et leur proposons une audition humaine.

Dans certains cas, nous devons **remettre** aux personnes les données personnelles qu'elles nous ont communiquées, en vue de leur réutilisation.

Nous veillons à ce que ces droits soient respectés !

7 Nous ne nous basons pas sur le consentement ☑

En principe, nous ne nous basons pas sur le consentement. Si c'est le cas, il doit être **volontaire** et **éclairé**. En cas de données sensibles[2] et de profilage à risque élevé, il doit être explicite.

10 Analyse d'impact relative à la protection des données (AIPD)

Pour les projets pouvant présenter un **risque** pour les personnes en termes de traitement des données, nous procédons à une AIPD. Nous y décrivons le projet et les mesures de protection, et vérifions s'il reste malgré tout des risques élevés en termes de **conséquences négatives** indésirables pour elles (le cas échéant : demander conseil). Nous conservons les AIPD.

8 Privacy by default

Lorsque nous avons des **paramètres** de confidentialité sur des sites web, apps, etc., ils sont **prédéfinis** au **minimum**. Nos développeurs y veillent.

9 Petit secret professionnel

Indique que la violation intentionnelle est punissable (jusqu'à CHF 250 000, sur plainte).

Nous gardons secrètes les données personnelles qui nous sont **confiées** et qui sont nécessaires à l'exercice de notre profession, ou nous indiquons clairement au préalable que nous ne les garderons pas secrètes.

Nous avons quelqu'un qui sait ce qu'il faut faire quand... 6 7 10 4

... une personne veut consulter/obtenir ses données ou les faire effacer ou rectifier ou a une autre préoccupation concernant la protection de ses données :

... nous avons un projet nouveau ou modifié qui concerne également des données de personnes et qui doit donc faire l'objet d'une vérification de la protection des données (év. avec AIPD) :

... des données personnelles sont perdues, tombent entre de mauvaises mains, ont été manipulées, que cela ait pu se produire ou qu'il y ait d'autres problèmes de sécurité :

Chacun signale immédiatement de tels incidents à cette personne !

[1] nLPD : https://fedlex.admin.ch/eli/fga/2020/1998/fr
[2] Données personnelles sensibles : Art. 5 let. c nLPD
[3] Voir modèle de pol. de confidentialité : https://dsat.ch
[4] Modèles : https://dsat.ch, https://bit.ly/3qrpOlb (DE)
[5] Voir Annexe 1 de l'OPDo (https://bit.ly/3VRjHKS)
[6] Voir FAQ (avec sources) : https://bit.ly/3MIb1TE (EN)
[7] Voir TIA : https://bit.ly/3L3mxYO (avec réf. au FAQ)

Questions ?

(FAQ : https://bit.ly/3EOsiIL et plus : https://bit.ly/3RCmuFQ)

Interne :

Externe : (peut engendrer des frais)

Lég. : Traitement des données | Gestion | Droits des pers. concernées | Processus | 4 Prio implémentation | ☐ Mis en oeuvre O/N

Sanctions pénales

La nLPD est plus stricte que le RGPD ou exige d'autres procédures incompatibles

Version 23.12.2022 – Mises à jour : www.rosenthal.ch

Auteur : David Rosenthal, drosenthal@vischer.com Trad. : Samira Studer et Julie Nikles

by VISCHER