REDstone consulting

LIGNES DIRECTRICES nLPD

Généralités

La nouvelle loi sur la protection des donnée (ci-après : nLPD), est en vigueur depuis le 1er septembre 2023 sans délai de mise en application.

La nLPD s'applique à **toutes personnes privées et aux organes fédéraux** qui traitent des données personnelles.

Une donnée personnelle est toute information liée à une personne (physique) identifiée ou identifiable, directement ou indirectement. Le traitement est toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés.

Se mettre en conformité ?

Notre méthodologie de contrôle propose se décline en trois catégories : **légal**, **gouvernance** et **cybersécurité**, parmi lesquelles nous avons identifié **11 domaines** (cf. verso) afin de vous aider dans votre processus de maturité nLPD.

01

Audit

- Evaluer l'état de maturité
- Recommandations pour combler les lacunes identifiées

02

Projet de mise en conformité

- Prioriser les points urgents audités

03

Processus de maintien de la conformité

- Dès la conception et par défaut
- Evolutions jurisprudentielles et législatives

RED

Esplanade de Pont-Rouge 4
1212 Lancy

+41(0) 78 762 77 81

info@redstoneconsulting.ch

www.redstoneconsulting.ch

11 domaines

1. Sensibilisation et formation *(gouvernance)*

Formation et sensibilisations instituées :

- Participation effective de tous les employés annuellement ;
- Formation spécifique et ciblées pour les métiers qui traitent des données sensibles.

2. Stratégie et gouvernance *(gouvernance)*

Désignations des ressources chargées de gérer la stratégie de protection des données :

- Si des traitements à risques sont effectués, alors il est conseillé de nommer un DPO ;
- Comité de protection des données crée avec le juridique et l'informatique;
- Rapports de conformité à la direction.

3. Registre de traitements *(gouvernance)*

Etablissement et revue annuelle du registre d'activités de traitements :

- Identification : données, y compris sensibles, traitements et leurs systèmes, acteurs source, transferts, motifs justificatifs, … ;
- Documenter les décisions automatisées et les profilages ;
- Évaluation en cas d'utilisation de l'intérêt légitime comme motif justificatif.

4. Revue contractuelle *(légal)*

Cadrer et contractualiser en cas de transfert de données à des tiers (par ex. des sous-traitants) :

- Inventaire des tiers ;
- Revue des contrats ;
- Accord interentreprise.

5. Processus métier *(gouvernance)*

Les processus métiers sont revus pour respecter les principes de protection des données :

- Documents et processus examinés, accessibles et connus des employés ;
- Si nécessaire, journalisation en place.

6. Politique de Confidentialité *(légal)*

Politiques de Confidentialité accessibles, compréhensibles, concises, conformes, à jour et documentées :

- Politique des employés vérifiés
- Politique des sites internet vérifiés
- Bandeaux de cookies installés

7. Droits des personnes *(gouvernance)*

Répondre à toutes les demandes dans les délais légaux :

- Un processus de demande de la personne concernée (DSAR) est documenté et utilisé.

8. Sécurité des données *(cybersécurité)*

Disponibilité, confidentialité, intégrité, traçabilité des données garanties, dès la conception et par défaut, par des mesures techniques et organisationnelles :

- Gestion des accès ;
- Transfert et stockage sécurisés ;
- Sauvegarde et test de restauration ;
- Chiffrement, anonymisation et pseudonymisation évalués ;
- Systèmes informatiques à jour ;
- Journaux d'accès pour l'identification et la qualification d'une violation de données ;
- Evaluation des risques de sécurité de l'information et existence d'une feuille de route.

9. Cycle de vie des données *(gouvernance)*

Protection de la collecte, au traitement, à la destruction :

- Etablir une politique de destruction et de rétention, régulièrement revue, selon les délais de prescriptions légaux.

10. Gestion des risques *(gouvernance)*

Gérer les risques liés à la protection des données pour les traitements à risques élevés pour les personnes concernées.

- Mesures pour contrôler et évaluer la gestion des risques ;
- Analyses de risque et d'impact (DPIA) ;
- Plans d'atténuation et des contrôles instaurés et surveillés pour chaque risque identifié.

11. Gestion des violations *(cybersécurité)*

Définir un plan d'incident mise à jour en cas d'incident :

- Définir la communication avec les parties prenantes ;
- Identification et classification des incidents, spécifiez les coordonnées des personnes compétentes ;
- Respect des délais de notification ;
- Décrire et documenter le processus de gestion des incidents ;
- Test de processus effectué périodiquement.

Conséquences en cas de violation ?

Mise en conformité interne
11 domaines

Recommandations non contraignantes
du Préposé fédéral (PFPDT) en cas de non respect des prescriptions

Procédure pénale sur plainte
contre une personne physique

SANCTION
Amende pouvant aller jusqu'à CHF 250'000.-