

s a n **j** c o

partenaire de votre développement



Plaque d'information pour les clients

Mise à jour de la loi fédérale sur la protection des données du 01.09.2023

Pourquoi une nouvelle loi sur la protection des données ?



La numérisation est plus que jamais un sujet d'actualité. C'est notamment l'une des raisons pour lesquelles le Conseil fédéral a entrepris la révision de la loi fédérale sur la protection des données (LPD), dont la nouvelle version entrera en vigueur le 01.09.2023. Le but de cette révision est principalement l'amélioration du traitement des données personnelles des citoyens suisses, ainsi qu'une redéfinition plus étayée de leurs droits propres. Ces changements amènent *de facto* avec eux un nombre important de nouvelles obligations, auxquelles les entreprises doivent se soumettre.

La nouvelle loi sur la protection des données (nLPD) s'appuie sur les dispositions précédemment adoptées par l'Union européenne en matière de droits des données personnelles. Elle se base également sur les avancées technologiques récentes, en intégrant dans ses champs d'application les outils de *cloud computing* ou de *big data* par exemple.

Cette nouvelle législation concerne ainsi de fait toutes les entreprises (petites et moyennes comprises) dont les travaux touchent au traitement ou à l'utilisation de données personnelles. Bien qu'elle demande des entreprises une forte implication et des mises à niveau pouvant être lourdes, elle offre également à ces dernières une opportunité unique d'optimiser leurs systèmes d'archivages et de protection des documents et données.



Dans les faits, qu'est ce qui change avec la nouvelle LPD ?



1 Modification du champ d'application

La nouvelle LPD ne couvre plus que les données des personnes physiques, à défaut des personnes morales.

2 Redéfinition des données sensibles

Les données génétiques et biométriques viennent s'ajouter à la liste des données sensibles, au même niveau que les mesures pénales par exemple.

3 Introduction des principes de « Privacy by Design » et « Privacy by Default »

Comprendre ici la protection de données dès la conception de ces dernières (*Design*) et également par défaut, lors de leur mise en circulation, sans intervention des utilisateurs (*Default*).

4 Devoir d'analyse et de contrôle

Il est nécessaire de mener des analyses permettant de déceler des éventuels problèmes dans des cas sensibles concernant la personnalité. Les entreprises surveillent également le traitement des données personnelles auprès des sous-traitants.

5 Devoir d'information

Les entreprises doivent informer les personnes à l'avance de la collecte de leurs données. Ceci ne s'applique plus uniquement aux données sensibles, mais à tout type de données personnelles.

6 Registre des activités de traitement

Les entreprises doivent nommer un responsable du traitement des données personnelles, lequel tient un registre des activités de traitement. Ce dernier décrit les étapes, processus et fins du traitement des données à l'interne.

7 Devoir d'annoncer

En cas de constat de violation ou entraves à la sécurité des données, une annonce rapide est à adresser à l'autorité compétente au niveau fédéral.

8 Introduction du principe de profilage

Définition de profilage dans son sens de « traitement automatisé des données personnelles des utilisateurs ».



Quelles mesures prendre dans les entreprises ?



Les mesures suivantes doivent être mises en place dans les entreprises :

- ❖ Dresser l'inventaire des activités de traitement des données personnelles et en nommer un responsable.
- ❖ Tenir un registre détaillé des activités de traitement de données.
- ❖ Évaluer et traiter les risques de fuites / pertes de données.
- ❖ Renforcer la prise de conscience du personnel et assurer la transparence dans le traitement des données.
- ❖ Garantir la sécurité informatique, tant hardware que software, et renforcer les droits et modes d'accès aux données.
- ❖ Définir des processus internes et vérifier l'adéquation des contrats et conditions générales à la nLPD.
- ❖ Assurer la formation initiale et continue du personnel ainsi que son information au sujet des normes de protection des données.

Sanjco SA permet aux entreprises d'atteindre ces objectifs, notamment par ses compétences dans les domaines suivants :

- ❖ Audit de la situation actuelle et recommandations de nos experts sur les points d'amélioration administratifs, procéduraux et juridiques.
- ❖ Analyse des données sensibles rattachées aux ERP et systèmes d'information en adéquation avec la nLPD.
- ❖ Tests d'intégrité et sécuritaires, analyse de l'infrastructure et des accès et recommandations d'amélioration.
- ❖ Implémentation de solutions de GED (Gestion électronique des documents) et ECM (Gestion de contenu d'entreprise) permettant une protection optimisée et cryptée des données et documents.

