# PROTECTION DE LA VIE PRIVÉE

10 étapes vers la nouvelle loi révisée sur la protection des données. Les violations intentionnelles des articles marqués **en rouge** sont passibles de sanctions. Les autres dispositions peuvent faire l'objet d'une action civile.

## 01 LISTE DES TRAITEMENTS DE DONNÉES

**Art. 12** Etablissez une liste des processus et activités dans le cadre desquels votre/vos organisation(s) traite(nt) des données personnelles (par ex. vente, cookies, marketing, service après-vente, location, dépannage, comptabilité, gestion du personnel, e-shop, vidéosurveillance). **La liste contient :** au moins le traitement, le but, les personnes de la catégorie, les données de la catégorie, le destinataire / le responsable du traitement, la durée de conservation. Eventuellement d'autres informations selon les besoins.

## 02 DÉCLARATION DE PROTECTION DES DONNÉES - DSE

**Art. 19** Chaque fois que vous collectez ou traitez des données personnelles qui ne sont pas requises par la loi, vous devez en informer de manière transparente dans la DSE avant le traitement. Le mieux est de mettre la DSE sur le site web, des liens vers celle-ci près des caméras vidéo, dans les contrats (renvoi à la DSE), les candidats, DSE séparée dans le règlement du personnel.

**La DSE contient :** vos coordonnées, la finalité du traitement des données, les catégories de destinataires, le transfert à l'étranger (pays), les droits des personnes concernées.

## 03 CONTRAT DE SOUS-TRAITANCE - ABV

**Art. 9** La plupart des entreprises donnent ou confient également l'accès aux données à des tiers, par exemple à des fournisseurs informatiques, au marketing, etc. Le sous-traitant ne peut faire que ce que nous sommes autorisés à faire. **Il faut donc conclure un "ABV" avec les tiers, un contrat qui établit votre souveraineté sur les données et qui oblige le tiers à respecter la protection et la sécurité des données.** Un CCA conforme au droit européen avec une référence à la LPD est suffisant. (Modèle : par exemple auprès de la Datenschutzstelle Liechtenstein).

## 04 SÉCURITÉ DES DONNÉES - TOMs & DSFA

**Art. 8** Nous protégeons les données personnelles par des mesures techniques et organisationnelles. **Techniquement** : accès uniquement avec un compte personnel et "MFA", accès de tiers uniquement sur demande et avec piste d'audit, pare-feu, logiciel antivirus, sauvegardes. **Organisationnel** : clean-desk, need-to-know, obligation de protection des données et formation, déchiquetage, etc. **Obligation de notification : art. 24**, si des données ont été perdues, il faut envisager une notification au PFPDT, edoeb.admin.ch. et envisager également une notification aux personnes concernées.

**Art. 22** Si l'organisation traite un grand nombre de données personnelles, des données très sensibles ou sensibles et que des erreurs ou d'autres risques pourraient présenter un risque pour la personne concernée, une analyse d'impact sur la protection des données - AIPD (risk assessment) doit être réalisée et documentée. L'AIPD **permet de vérifier de manière approfondie si les mesures prises pour protéger les données personnelles sont réellement appropriées**.

## 05 TRANSMISSION À L'ÉTRANGER

**Art. 16** Pas de pays étranger et donc **pays vers lesquels des données personnelles peuvent être transférées :** l'UE, le Royaume-Uni, l'EEE et certains autres pays de la liste des pays. N'oubliez pas que ces pays doivent être mentionnés dans la DSE.

Dans d'autres pays, les données peuvent être traitées si cela est nécessaire et stipulé dans un contrat au cas par cas. La personne concernée a renoncé à une protection séparée ou **il existe ce que l'on appelle des CCS, c'est-à-dire des clauses contractuelles standard de l'UE avec référence à la Suisse**.

## 06 DROITS DES PERSONNES CONCERNÉES

**Art. 25 et suivants** Nous accordons aux personnes concernées les droits mentionnés dans la DSE, à savoir **l'accès à** leurs propres données personnelles (pas les documents) et, sur demande, à d'autres informations. La loi accorde un délai de 30 jours pour l'accès gratuit. Auparavant, nous devons identifier la personne qui demande les informations. Attention, un renseignement faux ou incomplet est punissable. Le but du renseignement doit être la protection de la personnalité. Les autres droits sont les suivants : **Autorisation** de données erronées. L'**effacement** ne peut être exigé que si nous n'avons pas de meilleure raison ou une obligation légale. Dans le cas d'une **décision entièrement automatisée**, **art. 21**, c'est encore un être humain qui décide sur demande.

## 07 PRINCIPES DE PROTECTION DES DONNÉES

**Art. 6** Nous appliquons dans nos processus au sein de l'organisation les principes relatifs à la protection des données : **licéité, bonne foi, limitation des finalités, obligation d'effacer les données, exactitude, transparence et sécurité des données.**

L'organisation documente ces principes et les procédures de respect des obligations de diligence raisonnable.

## 08 PROTECTION DE LA VIE PRIVÉE PAR DÉFAUT

**Art. 7** Lorsque nous donnons un choix à une personne concernée, les paramètres de confidentialité et de sécurité d'un système, d'une application ou d'un produit doivent être réglés **par défaut sur les** options **les plus sûres ou les plus respectueuses de la vie privée**.

## 09 PETIT SECRET PROFESSIONNEL

**Art. 62** Les données personnelles qui ont été transmises à l'organisation doivent être tenues confidentielles, sauf avis contraire de la personne concernée.

## 10 FORMATION DU PERSONNEL

Les collaborateurs jouent un rôle très important dans la mise en œuvre et le respect de la protection des données. Il y a de nombreuses raisons pour lesquelles les employés doivent être formés à la protection des données :

**Éviter les sanctions** : Les infractions aux lois sur la protection des données peuvent entraîner des sanctions personnelles importantes pouvant aller jusqu'à 250 000 CHF.

**Sécurité des données** : les employés formés sont mieux préparés à identifier et à éviter les risques de sécurité potentiels, tels que les attaques de phishing, les mots de passe non sécurisés et autres problèmes de sécurité.

**La confiance des clients** : Les clients sont plus susceptibles de faire confiance aux entreprises qui protègent leurs données. De bonnes pratiques en matière de protection des données peuvent contribuer à la satisfaction des clients.

*Il s'agit d'une information abrégée sur la nouvelle loi sur la protection des données, elle ne comprend que le minimum et n'aborde pas les succursales, les autres domaines d'activité, etc. et ne constitue pas un conseil juridique.*

Auteur : impunix AG, Lagerhausstrasse 18, 8400 Winterthur ; info@impunix.ch