PROTECTION DES DONNÉES

01 LISTE DES TRAITEMENTS DE DONNÉES

Art. 12 Dressez la liste des processus et activités dans le cadre desquels votre/vos organisation(s) traite(nt) des données personnelles (par ex. vente, cookies, marketing, après-vente, location, dépannage, comptabilité, gestion du personnel, boutique en ligne, vidéosurveillance). **La liste contient :** au moins le traitement, le but, la catégorie de personnes, la catégorie de données, 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 placer la DSE sur le site web, de créer des liens vers celle-ci pour les caméras vidéo, dans les contrats (référence à la DSE). Pour les candidats et les employés, il est recommandé d'avoir une DSE séparée dans le règlement des employés.

03 CONTRAT DE SOUS-TRAITANCE - ABV

Art. 9 La plupart des entreprises donnent ou confient l'accès aux données à des tiers, par exemple à des fournisseurs de services informatiques, au marketing, etc. Le sous-traitant ne peut faire que ce que nous sommes autorisés à faire. **Il est donc nécessaire de conclure un "ABV" avec les tiers, un contrat qui établit votre souveraineté sur les données et oblige le tiers à respecter la protection et la sécurité des données.** Un ABV conforme au droit de l'UE avec une référence à la DSG est suffisant (modèle : par exemple, auprès de l'Agence de protection des données du 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 un "MFA", accès de tiers uniquement sur demande et avec une piste d'audit, pare-feu, logiciel antivirus, sauvegardes. **Organisationnel** : clean-desk, need-to-know, engagement de protection des données et formation, déchiquetage, etc. **Obligation de notification Art. 24 :** Si des données ont été perdues, une notification au PFPDT (edoeb.admin.ch) et, le cas échéant, une notification aux personnes concernées doivent être envisagées.

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

05 TRANSFERTS VERS L'ÉTRANGER

Art. 16 Pas de pays non sûrs 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, si la personne concernée a renoncé à une protection séparée ou **s'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 (autres que les documents) et, sur demande, à d'autres informations. La loi prévoit un délai de 30 jours pour l'accès gratuit. Avant cela, nous devons identifier la personne qui demande les informations. Attention : une information fausse ou incomplète est punissable. Le but de l'information doit être la protection de la personnalité. Les autres droits sont les suivants : **Rectification** des données erronées. **L'effacement** ne peut être demandé que si nous n'avons pas de meilleure raison ou si la loi l'exige. Dans le cas d'une **décision entièrement automatisée** (**art. 21**), un être humain peut encore prendre une décision sur demande.

07 PRINCIPES DE PROTECTION DES DONNÉES

Art. 6 Nous appliquons les principes de protection des données dans nos processus au sein de l'organisation : **légalité, bonne foi, limitation des finalités, obligation d'effacement, exactitude, transparence et sécurité des données.** L'organisation documente ces principes et les procédures de respect des obligations de diligence.

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**.

09 SECRET PROFESSIONNEL

Art. 62 Les données personnelles remises à l'organisation doivent être tenues confidentielles, sauf avis contraire de la personne concernée.

10 FORMATION DU PERSONNEL

Les employés jouent un rôle très important dans la mise en œuvre et le respect de la protection des données. Il existe 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 très abrégée sur la nouvelle loi sur la protection des données et non d'un conseil juridique.

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.

impunix
einfach datenschutz

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