Association Professionnelle Suisse
APS TSO
Techniciens en salle d'opération diplomés ES
Dipl. Fachfrauen/-männer Operationstechnik HF
Tecnici di sala operatoria diplomati SSS

# Fiche d'information sur la protection des données
# Mise en œuvre de la nouvelle loi sur la protection des données à partir du 1er septembre 2023

## Pour les organisations, les employés ou les indépendants qui traitent principalement des données personnelles sensibles (p. ex. des données relatives à la santé).

### 1. Protection des données / Résumé introductif

La loi fédérale sur la protection des données actuelle (LPD; en vigueur depuis 1992) ainsi que l'ordonnance y afférente ont pour but de protéger la personnalité et les droits fondamentaux des personnes physiques dont les données personnelles sont traitées.

Cette fiche d'information montre ce que signifie la protection des données et ce que cela implique en particulier pour les personnes responsables qui travaillent avec des données personnelles sensibles (surtout des données relatives à la santé) ou qui traitent de telles données.

La nouvelle loi sur la protection des données, qui entrera en vigueur le 1er septembre 2023, assure une protection encore meilleure des données personnelles. Les principales nouveautés, comme notamment le développement des "données sensibles", le "profilage à risque élevé»", la "protection des données dès la conception et défaut", la déclaration de protection des données sur le site web, le registre des activités de traitement dans certains cas ou les amendes sont abordées ci-dessous.

Ceux qui ont déjà traité correctement les données personnelles conformément à la loi sur la protection des données en vigueur ne rencontreront pas de problèmes majeurs avec la nouvelle loi sur la protection des données. Il convient néanmoins de tenir compte des points suivants:

### 2. Objectif et finalité de la protection des données

La protection des données traite de l'autodétermination informationnelle et de la protection contre le traitement abusif des données qui limite les personnes physiques dans leur personnalité ou leurs droits fondamentaux. La loi sur la protection des données a toujours eu pour but de protéger ces droits en définissant des directives sur l'utilisation et le traitement des données personnelles.

### 3. Nouvelle loi sur la protection des données (LPD) à partier du 1er septembre 2023

Le 1er septembre 2023, la loi sur la protection des données (LPD) totalement révisée, les dispositions d'exécution dans la nouvelle ordonnance sur la protection des données (OPDo) ainsi que la nouvelle ordonnance sur les certifications en matière de protection des données (OCPD) entreront en vigueur.

La loi révisée sur la protection des données et les dispositions correspondantes dans les ordonnances assureront à l'avenir une (encore) meilleure protection des données personnelles. La

protection des données est notamment adaptée aux évolutions technologiques, l'autodétermination concernant les données personnelles est renforcée et la transparence lors de la collecte de données personnelles est accrue.

La nouvelle loi sur la protection des données assure ensuite en particulier la compatibilité avec le droit européen (RGPD). Les adaptations apportées au nouveau droit de la protection des données sont importantes pour que l'UE continue de reconnaître la Suisse comme un pays tiers disposant d'un niveau de protection des données adéquat et pour que la transmission transfrontalière de données reste possible à l'avenir sans exigences supplémentaires.

### 3.1 Qu'est-ce qui reste inchangé ?

Le mode de traitement des données selon la nouvelle loi sur la protection des données ne change pas fondamentalement. Comme jusqu'à présent, le traitement de données personnelles générales ne nécessite pas de consentement explicite ou d'autre motif justificatif, pour autant que:

- les principes de traitement de la transparence - notamment le respect des obligations d'information-, de la finalité, de la proportionnalité ainsi que de la sécurité des données sont respectés,
- la personne concernée ne s'est pas opposée (au préalable) au traitement
- et qu'aucune donnée personnelle sensible n'est communiquée à des tiers.

Comme jusqu'à présent, un consentement explicite des personnes concernées n'est nécessaire au moment de la collecte des données que si des données personnelles sensibles sont traitées (p. ex. données relatives à la santé).

Il convient de veiller à ce que toutes les données à caractère personnel soient effacées ou rendues anonymes dès qu'elles ne sont plus nécessaires aux fins qui ont justifié leur traitement.

### 3.2 Principales modifications et nouveautés

- **Champ d'application personnel et matériel (art. 2 LPD)**

La nouvelle loi sur la protection des données (LPD) et l'ordonnance correspondante s'appliquent comme jusqu'à présent au traitement de données personnelles par des particuliers et des organes fédéraux. Par conséquent, les entreprises privées, mais aussi les associations et, en principe, les personnes privées qui traitent des données de personnes physiques sont concernées.

A l'avenir, la nouvelle LPD ne s'appliquera plus aux données des personnes morales. Par conséquent, seules les données des personnes physiques sont encore concernées et protégées.

- **Extension du catalogue des données personnelles dites "sensibles" (art. 5 LPD)**

Sont également considérées comme des données personnelles "sensibles" les données relatives aux opinions ou activités religieuses, philosophiques, politiques ou syndicales; les données relatives à la santé, à la sphère intime et à l'appartenance à une ethnie ou une race; les données relatives aux poursuites ou sanctions administratives et pénales ainsi que les données relatives aux mesures d'aide sociale.

Le catalogue actuel des données personnelles "sensibles" est élargi. Désormais, les données d'identification pouvant être saisies numériquement, telles que les données biométriques, les empreintes digitales, les données génétiques, scan rétien etc.

- **Profilage / profilage à risque élevé (art. 5 LPD)**

Le terme "profilage" est désormais utilisé, ce qui signifie tout traitement automatisé de données.

Le profilage désigne les données personnelles qui permettent de se faire une idée précise d'une personne. Il s'agit de caractéristiques telles que le lieu de résidence d'une personne, ses hobbies et ses intérêts. Mais il s'agit également de données telles que l'évolution des performances professionnelles, la situation économique ou des informations sur l'état de santé d'une personne.

On parle de "profilage à risque élevé" lorsqu'un profilage entraîne un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée en conduisant à une mise en relation de données qui permet d'évaluer des aspects essentiels (par ex. des traits de caractère) d'une personne physique. Il sera certes toujours possible à l'avenir de traiter de telles données avec un degré de sensibilité élevé, mais uniquement si elles ne portent pas expressément atteinte aux droits de la personnalité et si la personne concernée a donné son consentement explicite.

- **Protection des données dès la conception et par défaut (art. 7 LPD)**

Le principe de la "protection des données dès la conception (Privacy by Design)" signifie que les systèmes utilisés pour le traitement des données personnelles doivent être conçus dès le départ de manière à pouvoir respecter la protection des données.

Par le principe des "protection des données par défaut (Privacy by Default)", on entend que les responsables doivent choisir les paramètres par défaut du logiciel ou de l'appareil de manière à ce que le traitement des données personnelles soit limité au minimum nécessaire pour l'utilisation prévue (seuls les cookies absolument nécessaires au service peuvent être installés). Tous les logiciels, le matériel ainsi que les services doivent être configurés de manière à protéger les données et à préserver la sphère privée des utilisateurs.

- **Cookies**

La nouvelle loi sur la protection des données en Suisse n'apporte pas d'obligation pour les bannières de cookies, mais une obligation d'information sur l'utilisation des cookies (les bannières de cookies ou aussi les couches de cookies sont des outils utilisés sur les sites web et dans les applications pour obtenir le consentement des utilisateurs au traitement des données. Avec une telle bannière, les utilisateurs doivent être en mesure d'accepter ou de refuser les cookies de manière ciblée). La Suisse ne reprend donc pas la directive européenne sur les cookies. Par conséquent, il est en principe conforme à la loi de ne pas installer de bannière de cookies sur les sites web suisses.

Toutefois, les exploitants de sites web suisses sont obligatoirement tenus d'informer sur l'utilisation de cookies, mais peuvent les créer de manière générale sans consentement explicite.

Si toutefois un trafic UE est généré sur le site web - c'est-à-dire que des produits/services sont également proposés à des personnes de l'UE - alors une bannière doit impérativement être mise en place pour être en conformité avec le RGPD (cf. point 3). En cas de doute, il est recommandé de mettre en place une bannière correspondante (p. ex. dans les cas de frontaliers ou de congrès internationaux).

- **Obligation d'informer lors de la collecte de données personnelles, déclaration de protection des données (art. 19 LPD)**

L'obligation d'information est renforcée par rapport à la législation actuelle. Désormais, les responsables doivent informer les personnes concernées de manière adéquate pour chaque collecte de données, et non plus seulement pour les données sensibles comme c'était le cas jusqu'à présent.

La nouvelle loi sur la protection des données ne contient pas de liste exhaustive de toutes les informations obligatoires qui doivent être communiquées à la personne concernée lors de la collecte. Au moins les informations suivantes doivent être communiquées obligatoirement:

- l'identité et les coordonnées du responsable au sein de l'entreprise/de l'association ou de l'indépendant qui traite les données
- les finalités du traitement
- En cas de communication de données : les destinataires ou les catégories de destinataires
- en cas de communication de données à l'étranger, en plus : l'État ou l'institution internationale et, le cas échéant, la garantie d'une protection appropriée des données ou l'exception si de telles garanties ne sont pas données
- en cas de collecte indirecte de données (c'est-à-dire de données qui ne sont pas collectées auprès de la personne concernée elle-même, en plus : les catégories de données personnelles traitées)
- l'exécution de décisions individuelles automatisées, c'est-à-dire une décision fondée exclusivement sur un traitement automatisé et entraînant des conséquences juridiques pour la personne concernée ou l'affectant de manière significative.

La LPD ne précise pas de quelle manière l'information doit être fournie à la personne concernée. Aucune exigence légale de forme ne s'applique, mais il convient de choisir une forme appropriée qui réponde à l'objectif d'un traitement transparent des données. A cet effet, il est recommandé de publier une déclaration de protection des données correspondante sur le site web.

Le formulaire de contact du site web doit impérativement indiquer à quelle fin les données personnelles fournies seront utilisées.

- **Registre des activités de traitement (uniquement) dans certains cas (art. 12 LPD)**

Les organisations de 250 collaborateurs et plus doivent tenir un registre de tous les traitements.

Les organisations de moins de 250 collaborateurs (c'est-à-dire les petites organisations/indépendants) ne doivent en tenir un que si elles traitent des données personnelles sensibles (p. ex. des données relatives à la santé).

Dans ce cas, le responsable doit tenir un registre de toutes les activités de traitement. Si le traitement des données est délégué à un sous-traitant, le responsable et le sous-traitant doivent chacun tenir un registre séparé :

- Le registre du responsable du traitement contient au moins les indications suivantes:

- l'identité du responsable
- la finalité du traitement

- une description des catégories de personnes concernées et des catégories de données personnelles traitées
- les catégories de destinataires
- dans la mesure du possible, le délai de conservation des données personnelles ou les critères de détermination de cette durée
- dans la mesure du possible, une description générale des TOM (mesures techniques et organisationnelles)
- en cas de communication de données personnelle à l'étranger, le nom de l'Etat concerné et les garanties prévu à l'art. 16 al. 2 LPD.

• En revanche, le registre du sous-traitant ne contient "que" des informations concernant:

- l'identité du sous-traitant et du responsable du traitement
- les catégories de traitements effectués pour le compte du responsable,
- les indications relatives aux TOM et, en cas d'échange de données avec l'étranger, les indications relatives à l'État

Les données personnelles traitées dans les cabinets médicaux ou dentaires, par exemple, comprennent notamment les données suivantes : les données de base et les données de contact des patients, des collaborateurs, des personnes de contact des prestataires de services ou d'autres établissements de santé (p. ex. nom, numéro de téléphone, adresse, adresse électronique ou encore date de naissance) ; les enregistrements relatifs au déroulement d'un traitement, les descriptions de symptômes, les diagnostics, les prescriptions, les réactions, les résultats de laboratoire, les radiographies, les médicaments, les données relatives à la sphère intime telles que l'état de santé, la vie sexuelle ou les sentiments, les données relatives aux collaborateurs et à la relation d'emploi, y compris les évaluations de performance et les fiches de paie (ces dernières sont également pertinentes pour les responsables RH internes).

- **Extension des droits des personnes concernées : droit à la restitution des données (art. 25 LPD)**

Outre l'obligation d'information, les droits des personnes concernées sont également étendus dans la LPD. Comme dans le RGPD, la personne concernée dispose désormais d'un droit à la remise et à la transmission des données. Les personnes concernées peuvent exiger que les données qu'elles ont communiquées leur soient remises dans un format électronique courant (dans un délai de 30 jours).

Dans tous les cas, les informations suivantes sont communiquées :

- l'identité et les coordonnées du responsable
- les données personnelles traitées en tant que telles
- les finalités du traitement
- la durée de conservation
- les informations disponibles sur l'origine des données personnelles

Si le responsable fait traiter des données personnelles par un sous-traitant, il reste tenu de fournir des informations.

Il est recommandé de préparer une procédure pour répondre rapidement aux éventuelles demandes des personnes concernées.

- **Notification des violations au PFPDT (art. 24 LPD)**

En vertu de la nouvelle LPD, les responsables doivent notifier le plus rapidement possible au PFPDT (Préposé fédéral à la protection des données et à la transparence) et à toutes les parties potentiellement concernées toute violation de la sécurité des données (p. ex. perte de données, cyberattaque) susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, afin d'éviter des sanctions ou d'autres complications.

- **Conseiller à la protection des données (art. 10 LPD)**

Les entreprises privées peuvent, à titre facultatif, nommer un conseiller à la protection des données conformément à l'article 10 LPD. Ceux-ci peuvent, mais ne doivent pas nécessairement, être liés à l'entreprise par un contrat de travail.

Les conseillers à la protection des données doivent être autorisés à faire connaître leur point de vue à la direction de l'entreprise en cas de divergence d'opinion. Les responsabilités en matière de protection des données et de sécurité de l'information peuvent ou doivent être réglées dans chaque entreprise indépendamment de la mise en place d'un conseiller à la protection des données au sens de l'article 10 LPD.

Si un conseiller en matière de protection des données est désigné, son nom et ses coordonnées doivent être indiqués dans la déclaration de confidentialité.

- **Punissabilité / Amendes**

En ce qui concerne la punissabilité, il faut notamment tenir compte du fait qu'à partir du 1er septembre 2023, la violation de certaines obligations entraînera une punissabilité qui n'affectera pas l'entreprise, mais la personne physique responsable. Les personnes responsables peuvent être aussi bien des membres de la direction que d'autres personnes habilitées à prendre des décisions au sein de l'entreprise ou encore les personnes qui ont commis une violation d'obligation (p. ex. violation du secret). En droit suisse, seule la commission intentionnelle est toutefois punissable.

En cas de violation de l'obligation d'informer, de renseigner et de collaborer (art. 60 LPD) ou de violation du devoir de diligence (art. 61 LPD), les personnes peuvent être condamnées à une amende pouvant atteindre 250 000 francs. Seule la commission intentionnelle est couverte, pas la négligence. L'intention est la réalisation de l'acte avec connaissance et volonté. Celui qui considère la réalisation de l'acte comme possible et s'en accommode (dol éventuel) agit déjà intentionnellement.

- **Responsabilité (à distinguer de l'amende pénale)**

Comme dans la LPD existante, mais à la différence du RGPD, ce n'est pas l'entreprise qui est responsable de la violation de la nLPD, mais la personne physique responsable de la violation au sein de l'entreprise.

Le message relatif à la nouvelle LPD précise toutefois que ce n'est pas le responsable de l'action qui est visé ici, mais le responsable de l'organisation. La responsabilité des personnes dirigeantes est clarifiée par la référence à l'art. 6 DPA dans l'art. 64 nLPD. C'est la seule façon de s'assurer que les personnes occupant des postes de direction sont responsables des violations et non l'employé fraîchement embauché.

## 4. Recommandations

- Vérification des paramètres (existants) relatifs à la Protection des données dès la conception et par défaut (art. 7 LPD) y compris les cookies, conformément (page 4)
- Vérification et adaptation de la/des déclaration(s) de protection des données sur le site web (pages 4/5).
- Vérifier que toutes les opérations de traitement des commandes par des tiers sont couvertes par des contrats
- Examen des responsabilités organisationnelles en matière de protection des données
- l'établissement d'un registre des traitements, si un tel registre est nécessaire (pages 5/6).
- Vérification de la documentation des mesures prises pour garantir la sécurité des données
- Définition des processus de traitement des demandes d'accès, de rectification et d'effacement et des oppositions au traitement des données
- Définition des processus de notification des violations de la sécurité des données (page 7)
- Définition des processus de suppression et d'archivage des données
- Informer les collaborateurs concernés de leur devoir de discrétion professionnelle