FIDUCIAIRE | SUISSE

Union Suisse des Fiduciaires

Protection des données dans le domaine fiduciaire

Une publication, un guide de :

INSTITUT FIDUCIAIRE ET DROIT

INSTITUT FIDUCIAIRE 4.0

Berne, août 2021

1. L'essentiel en bref

Le 25.09.2020, le Parlement a accepté la loi suisse sur la protection des données (LPD) totalement révisée. Il compte sur une entrée en vigueur de la loi en 2023 suite à l'élaboration de l'ordonnance correspondante.

La nouvelle loi suisse sur la protection des données réglemente plus en détail les points suivants : les données personnelles nécessitant une protection particulière, le profilage (évaluation automatique des données personnelles), le devoir élargi d'information, les droits des personnes concernées ainsi que les dispositions pénales.

Ce guide a pour objectif d'énumérer les points individuels auxquels vous devez prêter attention en ce qui concerne la nouvelle loi sur la protection des données et quelles mesures nécessaires vous devriez prendre. Il est également recommandé de procéder à un examen lorsqu'on a déjà mis en œuvre les mesures RGPD au sein de l'entreprise : en effet, certaines différences doivent être prises en compte.

2. Protection des données est synonyme de protection de la personnalité

La protection des données a pour objectif la protection de la personnalité et celle des droits fondamentaux des personnes pour lesquelles des données sont traitées. La protection est considérable : la totalité des données personnelles est protégée, c'est-à-dire toutes les informations et indications qui se rapportent à une personne identifiée ou identifiable ou qui peuvent être attribuées à une personne déterminée ou déterminable. Par traitement, on entend – indépendamment des moyens et procédures appliqués (physiquement ou électroniquement) – toute gestion de données personnelles (acquisition, enregistrement, stockage, utilisation, modification, communication, archivage, suppression, destruction, etc.). La nouvelle loi sur la protection des données se concentre sur les personnes physiques. Les données de personnes morales ne sont désormais plus protégées.

3. Principes pour le traitement des données

Les principes imbriqués suivants s'appliquent au traitement des données personnelles :

Légalité : les données ne peuvent être traitées que dans le cadre de ce qui est légalement admissible.

Bonne foi : le principe constitutionnel de la bonne foi s'applique à l'ensemble de l'ordre juridique et spécifie clairement dans le droit de la protection des données qu'un traitement abusif des données est inadmissible.

Proportionnalité : seules peuvent être traitées les données nécessaires au but poursuivi (prévention et minimisation des données), et uniquement la quantité requise à cet effet. Sur le plan organisationnel, les personnes et les organismes n'ont droit d'accéder qu'aux seules données qui sont nécessaires pour l'exécution de leurs tâches.

Affectation : tout traitement des données doit poursuivre un objectif déterminé (l'acquisition des données à titre préventif est inadmissible). Les données ne peuvent être traitées que dans le but prévu ou établi.

Transparence : les circonstances ou les informations explicites données à la personne concernée doivent lui suffire pour qu'elle sache quel type de traitement effectuer.

Prise en compte du respect de la vie privée par défaut et dès la conception (« *privacy by defaut and by design* ») : à l'aide de mesures techniques et organisationnelles, le principe de la protection des données par la technique et par les paramètres par défaut

respectueux de la protection des données vise à garantir le respect des principes de l'affectation et de la proportionnalité.

Exactitude : les données traitées doivent être exactes et complètes en ce qui concerne le but de leur traitement. Les données erronées doivent être rectifiées, supprimées ou détruites.

Sécurité : les mesures techniques et organisationnelles doivent garantir la sauvegarde des données traitées. Ces mesures doivent protéger les données, en particulier contre une modification, une suppression, une destruction non intentionnelles ou illicites, ou un accès non autorisé.

Le/la responsable de la protection des données décide du but et des modalités du traitement. La protection des données est donc l'affaire des chefs !

4. Traitement juridiquement conforme des données personnelles

Le traitement des données personnelles est juridiquement conforme lorsqu'il respecte les principes généraux du traitement des données ainsi que, le cas échéant, les exigences légales supplémentaires. Les trois violations suivantes des règles de la protection des données sont fréquentes dans la pratique :

1. Trop de données sont collectées.
2. Les données ne sont pas ou insuffisamment protégées contre un accès non autorisé ou contre une perte.
3. Les données erronées et celles qui ne sont plus nécessaires ne sont pas détruites.

Outre les prescriptions de la loi sur la protection des données, des dispositions légales spécifiques supplémentaires peuvent être applicables (p. ex. ordonnance concernant la tenue et la conservation des livres de comptes).

5. Catégories de données

On distingue deux catégories de données.

Données à caractère personnel :

Les données à caractère personnel comprennent toutes les informations qui se rapportent à une personne physique identifiée ou identifiable. Un lien doit donc être établi, directement ou indirectement, entre une information d'une part, et une personne d'autre part. Un lien direct est p. ex. établi par le biais du nom, de l'adresse ou de la date de naissance. Un lien indirect s'effectue p. ex. par le biais de connaissances supplémentaires, comme par exemple les numéros de téléphone, de matricule et d'assurance sociale, ou les identifiants en ligne tels qu'adresses IP et identifiants de Cookie. Pour ce faire, il suffit que l'information permette théoriquement d'identifier la personne concernée ; il importe donc peu que la personne soit réellement identifiée.

Les informations doivent se référer à un être humain vivant. Les informations détaillées sur des personnes morales, telles que des sociétés de capitaux ou des associations enregistrées, ne sont pas considérées comme des données à caractère personnel. Il n'en va différemment que si les indications se réfèrent également aux personnes qui se trouvent derrière la personne morale, c'est-à-dire qu'elles se répercutent sur ces personnes. Cela peut par exemple être le cas d'une S.à.r.l. créée par une personne individuelle ou d'une

société en raison individuelle, lorsqu'il existe des interdépendances étroites sur le plan financier, personnel ou économique entre la personne morale et la personne physique.

Catégories particulières de données à caractère personnel

Les catégories particulières de données à caractère personnel sont spécifiquement protégées. Il s'agit par exemple des données relatives à la santé, à l'origine ethnique ainsi qu'aux convictions religieuses ou idéologiques, et aux données salariales.

6. Communication et transmission des données

Communication des données à des tiers

La communication de données constitue un traitement des données et doit donc se conformer aux principes figurant dans la législation sur la protection des données. En particulier, une communication des données à des tiers non autorisés, ou en dehors de l'objectif poursuivi par la collecte des données, est inadmissible, pour autant que la personne concernée n'ait pas donné son consentement ou n'a pas été informée en conséquence. La communication de données personnelles qu'il faut particulièrement protéger, ou de profils de personnalités, est illicite lorsqu'il n'existe aucun intérêt prépondérant ou aucune base légale. (En outre, une obligation d'information s'applique ici lors de l'acquisition).

Traitement du mandat

Si les données sont traitées par un tiers sur mandat du/de la responsable, cette personne chargée de traiter le mandat est tenue de respecter les mêmes dispositions que le/la responsable. Par ailleurs, aucune obligation légale ou contractuelle de garder le secret ne doit être contraire au traitement du mandat.

Communication des données à l'étranger

Les données personnelles ne peuvent être communiquées à l'étranger que lorsque la législation de l'État en question garantit un niveau de protection adéquat. (Le PFPDT tient une liste correspondante des États assurant un niveau de protection correspondant). Exceptionnellement, lorsque des mesures de protection supplémentaires sont prises, une communication des données est possible à un pays qui ne dispose d'aucun niveau de protection adéquat.

Obligation de renseigner

Toute personne peut exiger des renseignements auprès du/de la responsable pour savoir si des données personnelles la concernant sont traitées. Le droit de demander des renseignements couvre toutes les informations nécessaires pour que la personne concernée puisse faire valoir ses droits en matière de protection des données. Le/la responsable peut exceptionnellement refuser ou limiter la communication d'un renseignement.

Obligation de rectifier

Le/la responsable doit rectifier les données inexactes sur demande de la personne concernée.

Obligation de restituer et de diffuser

La nouvelle loi sur la protection des données prévoit explicitement que toute personne peut exiger la restitution ou la diffusion de ses données personnelles, qu'elle a communiquées au/à la responsable, dans un format électronique courant.

Conseiller en matière de protection des données

La nomination d'un conseiller en matière de protection des données, qui sert de point de contact pour les personnes concernées ou pour les autorités, est facultative.

7. Sauvegarde des données

La sauvegarde des données consiste en des mesures techniques qui devraient être prises afin de protéger les données contre la perte, la manipulation, l'accès par des tiers, les virus, etc.

Les mesures techniques et de personnel destinées à protéger contre la perte de données et contre l'accès non autorisé dépendent de l'infrastructure informatique individuelle et relèvent, par conséquent, de la responsabilité de l'entreprise. Vous trouverez des détails sur ce sujet dans le guide pour la sécurité informatique (protection des données) en cliquant sur le lien suivant : https://bit.ly/30UayX3

En règle générale, les mesures prises en vue de garantir la sauvegarde des données soutiennent la protection des données. Toutefois, cela peut également conduire à de nouveaux conflits et questionnements. Ainsi, l'externalisation de la sauvegarde dans le nuage ou dans un système tiers peut impliquer des risques liés à la protection des données, puisque des données peuvent ainsi être consultées ou téléchargées par des personnes tierces non autorisées. Il convient d'enrayer ce problème en faisant appel à des mesures appropriées et en examinant cette question au préalable.

8. Conservation, restitution et destruction des données

Les entreprises ne peuvent collecter et traiter les données à caractère personnel qu'à des fins légitimes et univoques – ainsi le prévoit le principe de finalité. Concrètement, cela signifie que les données collectées doivent être supprimées ou éventuellement anonymisées aussitôt que l'objectif pour lequel elles ont été collectées – par exemple une réclamation – a été rempli. Si les données à caractère personnel sont soumises à un délai légal de conservation, elles ne doivent être supprimées qu'après expiration de ce délai de conservation. Dans la pratique, deux solutions viables se sont répandues jusqu'à présent. L'effacement (masquage) de données, ainsi que le cryptage / la restriction des droits d'accès avec une déclaration de consentement des personnes concernées. Fait la plupart du temps partie intégrante de CG ou de règlements du personnel, etc.

9. Nouvelles obligations en matière de gouvernance, d'information et de diligence

La nouvelle loi sur la protection des données, qui entrera probablement en vigueur en 2023, prévoit des obligations supplémentaires en matière de gouvernance et d'information au regard du droit actuellement en vigueur lors du traitement des données ; la violation intentionnelle de ces obligations pourra conduire à des amendes s'élevant jusqu'à 250 000 francs.

Registre des activités de traitement

En vertu de la nouvelle loi sur la protection des données, les responsables et les personnes chargées de traiter les mandats devront tenir un registre de leurs activités de traitement, qui doit comporter au moins les indications suivantes : l'identité du/de la responsable, le but visé par le traitement, la description des catégories, des personnes et des données personnelles concernées, les catégories des destinataires des données, le délai de conservation et les critères relatifs à la fixation de ce délai, la description des mesures garantissant la sauvegarde des données, l'indication de l'État et d'éventuelles garanties de protection lors d'une communication de données à l'étranger.

Obligation d'information

Celui qui prélève des données personnelles informe la personne concernée de manière adéquate au sujet de l'acquisition des données. L'information comprend au minimum l'identité et les coordonnées du/de la responsable, le but visé par le traitement et, le cas échéant, les tiers ou la catégorie de tiers auxquels les données personnelles ont été communiquées. L'obligation d'information disparaît lorsque la personne concernée dispose déjà des informations correspondantes, que le traitement est prescrit légalement ou que le/la responsable est légalement tenu/e au secret.

Analyse d'impact relative à la protection des données

Si le traitement de données personnelles implique un risque élevé pour la personnalité ou pour les droits fondamentaux de la personne concernée, le/la responsable doit préalablement établir son analyse d'impact relative à la protection des données avec une description du traitement prévu, une évaluation des risques et les mesures.

Obligation d'information

Il convient d'annoncer aussi rapidement que possible le PFPDT et, le cas échéant, la personne concernée, lors de violations de la sauvegarde des données qui impliquent probablement un risque élevé pour la personnalité et pour les droits fondamentaux de la personne concernée.

10. Conséquences juridiques en cas de violation de la protection des données ou des obligations administratives

Sous la loi de la protection des données actuellement en vigueur, les personnes lésées dans leur personnalité par un traitement illicite des données peuvent déposer une plainte civile afin de protéger leur personnalité et exiger en particulier que le traitement des données soit interdit, qu'aucune donnée ne soit communiquée à des tiers, ou que les données personnelles soient rectifiées ou détruites.

Outre les exigences de droit civil dans le cas d'une violation des obligations d'informer, de renseigner et de collaborer, ainsi que des obligations de diligence, la nouvelle loi sur la protection des données prévoit une responsabilité de droit pénal : des amendes s'élevant jusqu'à 250 000 francs menacent en cas de manquement intentionnel aux obligations.

11. « Best practice » dans l'entreprise fiduciaire : conseils pratiques

- S'assurer à l'aide de mesures simples contre le risque d'une violation de la protection des données
    - Réaliser un état des lieux propre de l'infrastructure informatique (en interne et en externe) afin d'identifier d'éventuels problèmes. Remédier à ces derniers lors d'une seconde étape.
    - Aborder le thème avec les clients, par exemple dans le sillage d'un entretien de clôture. Faire des propositions directes de solutions (p. ex. dans le cas d'un envoi de données non cryptées à caractère personnel)
    - Énumérer les domaines où surviennent des pièges potentiels (p. ex. comptabilité des salaires, archivage des documents comptables comportant des données à caractère personnel). Définir les opérations à effectuer dans ces cas de figure

  - Indiquer aux collaborateurs les dangers qui peuvent survenir dans la gestion de courriels et de terminaux mobiles. À cet égard, définir des solutions et des règles d'action
  - Établir des confirmations de mandat avec les passages correspondants relatifs à la protection et au stockage des données
- Exemples de négligence grave lors de la gestion de données chez un agent fiduciaire
  - Envoyer des données salariales non cryptées au client ou directement au collaborateur sans leur accord explicite
  - Accès à des données non régis sur la base de la compétence / responsabilité
  - Utilisation de solutions en nuage sans l'application d'une authentification à 2 facteurs (non-respect des principes relatifs à la sécurité fondée sur le nuage)
  - Aucune attention particulière n'a été portée à la protection de données à caractère personnel (enregistrées en interne ou en externe)

12. Informations complémentaires

- Site web du Préposé fédéral à la protection des données et à la transparence (PFPDT) : https://www.edoeb.admin.ch
- Charte de l'économie suisse pour une gestion responsable des données : www.economiesuisse.ch/fr/gestiondedonnees
- Liste PFPDT des États ayant une législation assurant un niveau de protection adéquat : https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2020/staatenliste.pdf.download.pdf/20200908_Staatenliste_f.pdf
- Guide de l'Institut FIDUCIAIRE 4.0 pour la sécurité informatique (protection des données) :https://www.fiduciaire40.ch/guide-pour-la-securite-informatique-protection-des-donnees