Webinaire
La protection des données du point de vue des PME

20 septembre 2023, 10h30-12h00

:

lic.iur.HSG Urs Freytag
Teufenerstrasse 3, 9000 St. Gall
Téléphone: 071 421 41 41
Mail: freytag@factum.pro

factum advocatur

SWISS MEDTECH

Contenu du webinaire

1 Partie théorique

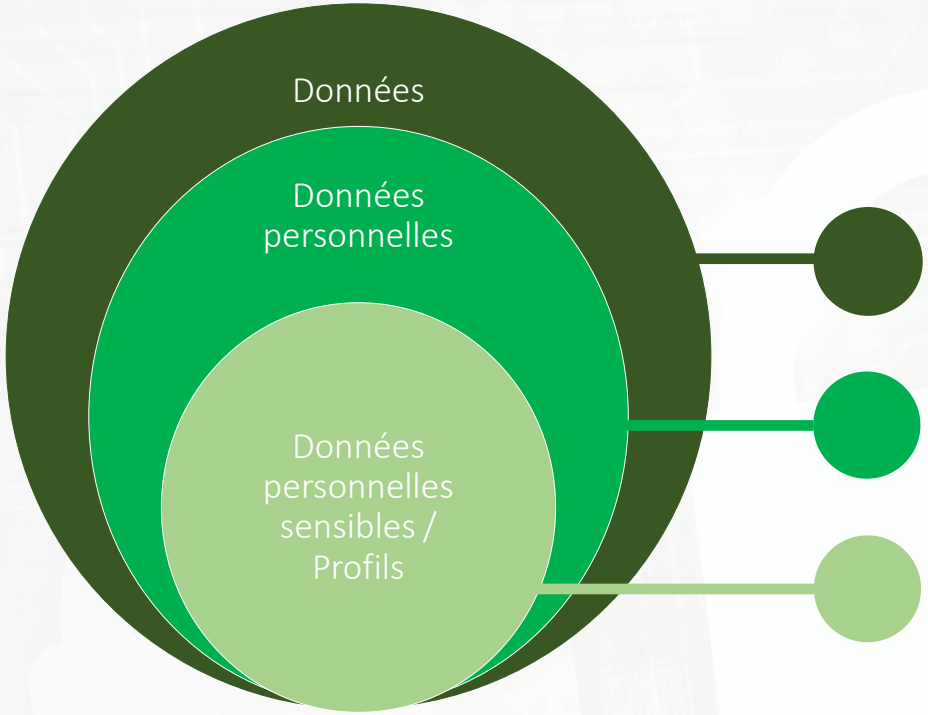
1. Définition – protection des données
2. Bases juridiques
3. Rapport entre la LPD et le RGPD
4. Principes de protection des données
5. Motifs justificatifs
6. Droits des personnes privées / Obligations des responsables du traitement des données
7. Profilage
8. Sanctions
9. Nouveautés dans la LPD

2 Mise en œuvre pratique

10. Déclaration de protection des données
11. Registre des activités de traitement
12. Sous-traitant
13. Conseiller / délégué à la protection des données
14. Protection des données dans le droit du travail
15. Mise en œuvre pratique – site web

3 Questions et réponses

1. Définition de la protection des données – Sphères



Toutes les données, même celles qui ne sont pas personnelles (par ex. données météorologiques, cours de la bourse, etc.)

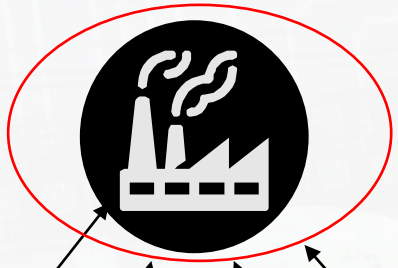
Données se rapportant à une personne **identifiée** ou **identifiable** (p. ex. nom, adresse, état civil, numéro de téléphone, sexe, numéro IP, etc.)

Données relatives à la santé, à la religion, à la vie privée, aux opinions politiques, aux données biométriques

Objectif de la protection des données : la protection de la *sphère privée* des personnes physiques contre les atteintes à la personnalité (et non la « protection des données »)

1. Définition de la protection des données – répartition des rôles

Personne **responsable** traitant des données
Organisation/État ; décide du but et des moyens



stocke des données

Sous-traitant (par exemple, société informatique, fournisseur de cloud, fiduciaire, entreprise de marketing, fabricant d'appareils de technologie médicale)

Sujets de données
(« personnes », p. ex. clients, travailleurs, citoyens)

Contrat de sous-traitant nécessaire

Microsoft

par ex. Microsoft 365

2. Bases juridiques de la protection des données

Suisse :

- Loi ou ordonnance sur la protection des données (LPD / OLPD)
- Lois cantonales sur la protection des données

  Traitement de données personnelles par les cantons et les communes

- Dispositions relatives à la protection des données dans d'autres lois (par ex. art. 328b CO – contrat de travail)

UE :

- Règlement général sur la protection des données (RGPD), en vigueur depuis le 25.05.2018
- Lois nationales sur la protection des données

Reste du monde :

- Lois nationales sur la protection des données

3. Rapport entre la LPD et le RGPD

Quand le RGPD est-il applicable en Suisse ?

Critères
- Principe fondé sur les cantons des succursales
- Principe fondé sur le lieu du marché

(Art. 3 RGPD)

Mais : la LPD CH s'applique de la même manière dans l'espace de l'UE lorsque des traitements de données de l'UE ont des répercussions en Suisse.

Schweizer Unternehmen:	Anwendbares Recht	
	CH DSG	EU DS-GVO
Hat Niederlassung in der EU	●	●
Bietet nur Leistungen in der Schweiz an	●	
Bietet Leistungen im EU-Raum an	●	●
Bearbeiten von Schweizer Personendaten	●	
Bearbeiten von Personen-daten von Betroffenen, die sich in der EU befinden	●	●

3. Rapport entre la LPD et le RGPD

LPD (Suisse)

« Autorisation avec réserve d'interdiction»

Le traitement des données est autorisé si les principes de protection des données (diapositive 8) sont respectés et si la loi n'interdit pas le traitement des données

RGPD (UE)

« Interdiction avec réserve d'autorisation »

Les traitements de données sont interdits s'ils ne sont pas autorisés par la loi, c'est-à-dire qu'il doit exister l'un des six motifs justificatifs (diapositive 10)

Renversement du fardeau de la preuve :

- Suisse (LPD) : celui qui fait valoir une violation de la protection des données doit en apporter la preuve
- RGPD : le responsable doit prouver la légalité du traitement des données

4. Principes de la protection des données (art. 6 – 8 LPD)

1. **Licéité** (art. 6, ch. 1)
2. **Proportionnalité / bonne foi** (art. 6, ch. 2)
3. **Finalité déterminée** (art. 6, ch. 3)
4. **Minimisation des données** (destruction ou anonymisation si elles ne sont plus nécessaires au regard des finalités) (art. 6, ch. 4)
5. Assurer l'**exactitude** des données (art. 6, ch. 5)
6. Si le **consentement** est requis, il doit être donné **volontairement** après une information appropriée (art. 6, ch. 6)
7. Consentement **exprès** en cas de données personnelles sensibles ou de profilage à haut risque (art. 6, ch. 7)
8. **Protection des données dès la conception** (« ***privacy by design »***) (art. 7)
9. **Protection des données par défaut** (**« *privacy by default »***) (art. 7)
10. **Sécurité des données** (art. 8)

! Les principes doivent être respectés. Le non-respect peut constituer une atteinte à la personnalité (art. 30, al. 2, LPD)

5. Justification du traitement des données (licéité)

Chapitre 5
Dispositions particulières pour le traitement de données personnelles par des personnes privées

Art. 30 Atteintes à la personnalité

1 Celui qui traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées.

2 Constitue notamment une atteinte à la personnalité le fait de:

a. traiter des données personnelles en violation des principes définis aux art. 6 et 8;

b. traiter des données personnelles contre la manifestation expresse de la volonté de la personne concernée;

c. communiquer à des tiers des données sensibles.

3 En règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement.

5. Justification du traitement des données (licéité)

Art. 31 LPD et art. 6 RGPD

Motifs justificatifs	Exemple :
1. **Consentement** de la personne concernée	Newsletter électronique
2. **Intérêt privé prépondérant**	Marketing direct, vérification de la solvabilité, ainsi que d'autres objectifs non liés à la personne (comme la recherche)
3. **Intérêt public prépondérant**	surtout des tâches étatiques (p.ex. Registre des habitants/données fiscales)
4. **Obligation légale**	Obligation de conservation des dossiers (10 ans)
5. **Exécution du contrat** (RGPD uniquement)	Offre / Livraison / Service
6. **Intérêts vitaux** (RGPD uniquement)	Traitement médical d'urgence

5. Justification du traitement des données (licéité)

Les activités de marketing sont-elles encore autorisées sans consentement ?

SUISSE: Art. 6 al. 7 ou art. 30 LPD :

Les traitements de données dans le cadre d'activités de marketing sont autorisés pour autant que les principes de la protection des données (diapositive 8) soient respectés.

Il ne doit cependant pas y avoir d'atteinte à la personnalité de la personne concernée (article 30 LPD).

UE (RGPD art. 6 f) :

Le traitement des données est autorisé lorsque le traitement est nécessaire aux fins des **intérêts légitimes poursuivis par le responsable du traitement**, à condition que ne **prévalent** pas les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel (...).

RGPD Considérant n° 47 (concernant l'article 6 f) : « Le traitement de données à caractère personnel à des fins de prospection peut être considéré comme étant réalisé pour répondre à un intérêt légitime. »

6. Droits des personnes privées / Obligations des responsables du traitement des données

1. Droit à **la transparence** par une déclaration de protection des données, art. 6 al. 3 LPD (finalité reconnaissable)
2. Droit à l'**information** lors de la collecte de données, art. 19 LPD
3. Droit de **savoir** si des données sont traitées, lesquelles et dans quel but, art. 25 LPD
4. Droit à la **remise** et à **la transmission des données**, art. 28 LPD
5. Droit de **rectification** (en cas de données erronées), art. 6, al. 5 / art. 32 LPD
6. Droit à l'**effacement** (« droit à l'oubli »), art. 6, al. 5 LPD
7. Droit de **contrôle** des décisions individuelles automatisées, art. 21, al. 2 LPD
8. Droit d'**opposition**

6. Droits des personnes privées / Obligations des responsables du traitement des données

NOUVEAU : réaliser une analyse d'impact relative à la protection des données personnelles (art. 22 LPD)

- Analyse préalable des risques en cas de risques présumés élevés pour la personne concernée
- Description du traitement prévu avec évaluation des risques pour les personnes concernées et des mesures à prendre pour la protection de la personnalité
- Ex. : Traitement de données sensibles à grande échelle
- Obligation d'informer le PFPDT si, malgré les mesures prises, le risque est élevé (art. 23 LPD)
    - L'obligation tombe si un conseiller à la protection des données a été engagé conformément à l'art. 10 LPD

NOUVEAU : obligation de notification en cas de violation de la sécurité des données (art. 24 LPD)

- par exemple après un piratage, dans la mesure où la violation entraîne vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée

7. Profilage (art. 5 let. f/g LPD)

Art. 5 let. f LPD : Le profilage désigne toute forme de traitement automatisé de données personnelles pour évaluer, analyser ou prédire certains **aspects personnels** concernant, par exemple, le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements.

Art. 5 let. g LPD : *Profilage* ***à risque élevé*** *: appariement de données qui permet d'****apprécier les caractéristiques essentielles de la personnalité*** *d'une personne physique.*

Quand y a-t-il un risque **élevé** ? Règle générale : Lorsque des déclarations sur la situation financière, la situation familiale, le niveau de formation, les opinions politiques, les activités de loisirs, etc., permettent de porter un jugement de valeur sur une personne

Le profilage à risque élevé n'est autorisé qu'avec un consentement exprès (art. 6, al. 7, LPD)

8. Sanctions

Suisse (LPD / DSG)

- Amendes de 250 000 francs au plus
- Le sujet de la sanction est le collaborateur responsable (!), donc une personne privée, et non l'entreprise

UE (RGPD)

- Amendes de 20 millions d'euros au plus
- ou 4 % du chiffre d'affaires annuel
- Le sujet de la sanction est l'entreprise

9. Nouveautés de la LPD révisée

- Entrée en vigueur **01.09.2023**
- Les principes de base de la protection des données restent les mêmes (licéité / finalité déterminée / proportionnalité, etc.)
- Obligations documentaires étendues (registre des activités de traitement ; exceptions pour les PME)
- Droits d'information étendus des personnes concernées
- Le consentement pour le traitement des données reste rarement nécessaire (contrairement au RGPD)
- Profilage à peine limité, mais introduction du profilage à risque élevé
- Simplification du transfert de données vers l'étranger
- Nouveau : fonction de conseiller à la protection des données (facultatif)
- Nouveau : dispositions pénales : amendes de 250 000 francs au plus / sujet de la sanction : personnes physiques (!)
- Davantage de compétences pour le Préposé fédéral à la protection des données (« PFPDT »)

PARTIE 2 : Mise en œuvre pratique

Clients / fournisseurs / collaborateurs existants (dans le CRM)

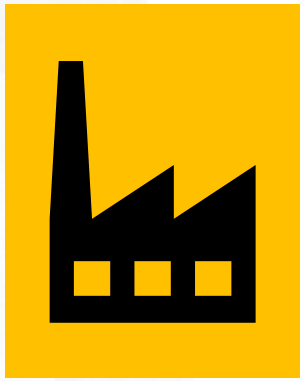
Relation contractuelle !

Intérêt privé prépondérant pour le marketing ?

Personnes connues par leur nom (pas dans le CRM)

Société XY

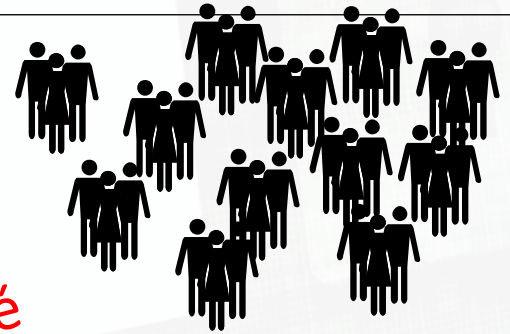
(responsable du traitement des données)



Système CRM

Consentement !

Contacts existants sans relation contractuelle, par ex. abonné à une newsletter (dans le CRM)



Intérêt privé prépondérant pour le marketing ?

Clients potentiels (pas dans le CRM)

Premier pas vers le succès : effectuer une analyse de la situation actuelle

1. Quelles sont les fichiers dont nous disposons ?
2. Quels sont les fichiers qui contiennent des données à caractère personnel ?
3. Où, par qui, dans quel but et pendant combien de temps conservons-nous ces données à caractère personnel ?
4. À qui transmettons-nous des données à caractère personnel ?
5. Qu’en est-il de la sécurité des données ?

10. Déclaration de protection des données

Devoir d'informer : art. 19 LPD : extension du principe de transparence

- L'information ***adéquate*** est une obligation légale (art. 19 LPD)
- **Sur quoi** faut-il informer ? Toutes les informations nécessaires pour permettre à la personne concernée d'exercer ses droits et pour garantir la transparence du traitement des données
- **Quand** faut-il informer ? Au moment de la collecte des données personnelles
- **Comment** informer ? La loi ne contient pas d'indications, habituellement par la publication d'une **déclaration de protection des données (DPD)**
- La DPD est une déclaration unilatérale et non un contrat
- Il doit pouvoir en être pris connaissance de manière simple et facilement accessible
- IMPORTANT : Le non-respect du devoir d'information est passible de sanctions (cf. art. 60 al. 1 LPD)

10. Déclaration de protection des données

Quel est le contenu minimal d'une DPD ?

- Identité et coordonnées du responsable
- Objectif et étendue du traitement des données (par ex. exécution du contrat)
- Destinataires ou catégories de destinataires auxquels les données personnelles sont communiquées
- Renvoi à des services intégrés de tiers tels que Facebook, LinkedIn, services Google, etc.
- Remarques sur l'utilisation de cookies

10. Déclaration de protection des données

Comment rédiger une DPD ?

- Clarification de la question préalable de l'applicabilité du RGPD
- Télécharger le modèle et l'adapter aux besoins individuels, par exemple

  http://www.dsat.ch/download

  http://www.weka.ch

  https://www.sgv-usam.ch/fr/grands-axes-politiques/politique-économique/sous-pages/nouveau-droit-de-la-protection-des-données
- Utiliser le générateur pour des DPD individuelles (par ex. https://brainbox.swiss/datenschutz-generator-schweiz/ [gratuit])
- Conseil par un cabinet d'avocats ou des entreprises spécialisées
- Solution entièrement automatisée avec un fournisseur externe
- Mise en ligne sur le site web (cliquable au niveau supérieur)

11. Registre des activités de traitement (art. 12 LPD/art. 30 RGPD)

Obligation de documentation pour **tous** les responsables du traitement et les sous-traitants (art. 12 LPD / art. 30 RGPD)

Comment établir un registre des activités de traitement ?

- La loi et l'ordonnance ne contiennent pas de directives
- Télécharger le modèle et l'adapter aux besoins individuels
- Conseil par un cabinet d'avocats ou une entreprise spécialisés
- Un registre suffit pour la LPD et le RGPD

11. Registre des activités de traitement (art. 12 LPD/art. 30 RGPD)

Art. 12 Registre des activités de traitement

[1] Les responsables du traitement et les sous-traitants tiennent chacun un registre de leurs activités de traitement.

[2] Le registre du responsable du traitement contient au moins les indications suivantes:

a. l'identité du responsable du traitement;

b. la finalité du traitement;

c. une description des catégories de personnes concernées et des catégories de données personnelles traitées;

d. les catégories de destinataires;

e. dans la mesure du possible, le délai de conservation des données personnelles ou les critères pour déterminer la durée de conservation;

f. dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données selon l'art. 8;

g. en cas de communication de données personnelles à l'étranger, le nom de l'État concerné et les garanties prévues à l'art. 16, al. 2.

[3] Le registre du sous-traitant contient des indications concernant l'identité du sous-traitant et du responsable du traitement, les catégories de traitements effectués pour le compte du responsable du traitement ainsi que les indications prévues à l'al. 2, let. f et g.

[4] Les organes fédéraux déclarent leur registre d'activités de traitement au PFPDT.

[5] Le Conseil fédéral prévoit des exceptions pour les entreprises qui emploient moins de 250 collaborateurs et dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées.

11. Registre des activités de traitement (art. 12 LPD/art. 30 RGPD)

Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
ABC Installation GmbH
Steinbauerstr. 45a
9999 Steinhausen

Tel. +41 999 99 99
E-Mail: team@abcinstallation.ch
Web: www.abcinstallation.ch

Verarbeitungs-tätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personen-bezogenen Daten	Kategorie von Emp-fängern	Drittlands-transfer	Aufbewahrungsdauer / Löschfristen	Technische/or-ganisatorische Massnahmen
Lohnabrech-nung	Hans Bauer 099 999 99 99 hans@abcinstallation.ch	02.03.2018	• Auszahlung der Löhne / Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name, Geburtsdatum • Adresse • Bankverbindungsdaten • Lohn-/Entgeltdaten • ggf. Religionszugehörigkeit • Sozialversicherungsdaten	Steuer-berater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheits-konzept
Personal-verwaltung	Hans Bauer 099 999 99 99 hans@abcinstallation.ch	02.03.2018	• Personaladministration • Personalführung • Arbeitszeitverwaltung • Personalbeschaffung (betrifft Bewerber)	• Beschäftigte • Auszubil-dende • Bewerber	• Name, Adressen • Zeitwirtschaftsdaten • Daten zur Arbeitsleistung • Leistungsbeurteilung • Lebenslauf und Bewer-bungsunterlagen (betr. Bewerber)	Keine	Keine	• Beschäftigte: in der Regel ca. 3 Jahre nach Aus-scheiden • abgelehnte Bewerber: 6 Monate nach Abschluss des Bewer-bungsverfah-rens	Siehe IT-Sicherheits-konzept
Betrieb der Firmenwebseite (über Hosting-Dienstleister)	Max Meier 099 999 99 98 max@abcinstallation.ch	28.02.2018	Aussendarstellung	• Webseiten-besucher	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheits-konzept + HTTPS-Verschlüsse-lung
Kunden-verwaltung	Jutta Klein 099 999 99 97 jutta@abcinstallation.ch	02.03.2018	• Bearbeitung von Aufträgen inkl. Rechnungstellung • postalische Werbung	• Kunden	• Name, Adresse • Angaben zum Auftrag • ggf. Bankverbindungsdaten	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheits-konzept

11. Registre des activités de traitement (art. 12 LPD/art. 30 RGPD)

Allégements pour les PME dans l'art. 24 de l'ordonnance relative à la LPD

– Art. 24 Exception à l'obligation de tenir un registre des activités de traitement

Les entreprises et autres organismes de droit privé employant moins de 250 collaborateurs au 1er janvier d'une année, ainsi que les personnes physiques, sont déliés de leur obligation de tenir un registre des activités de traitement, à moins que l'une des conditions suivantes soit remplie:

a. le traitement porte sur des données sensibles à grande échelle;
b. le traitement constitue un profilage à risque élevé.

12. Sous-traitant / Cloud

- Transmission de données à des tiers en vue de l'externalisation de traitements de données (art. 9 LPD).
- Les personnes concernées ne doivent pas être informées
- Exemples : solutions cloud (p. ex. OneDrive), fiduciaires, Mail-Chimp, etc.
- Prérequis :
  - Accord contractuel avec le sous-traitant sans forme particulière, donc également oral)
  - Respect des principes de protection des données par le sous-traitant
  - Pas d'obligation contractuelle ou légale de confidentialité
- Le sous-traitant ne peut traiter les données que comme le responsable du traitement serait autorisé à le faire
- IMPORTANT : le donneur d'ordre (responsable) reste dans tous les cas responsable du respect des dispositions relatives à la protection des données
- Besoin d'agir : vérifier si un sous-traitant est défini ou non
- Pour les grandes entreprises : les dispositions relatives à la protection des données sont déjà contenues dans ce que l'on appelle les clauses contractuelles standard ou les conditions générales.

13. Conseiller / délégué à la protection des données

Une entreprise a-t-elle besoin d'un délégué à la protection des données (RGPD) / d'un conseiller à la protection des données (LPD) ?

- LPD : **conseiller à la protection des données** -> est facultatif (art. 10 LPD)
  - Tâches : Point de contact pour les personnes privées et les autorités concernées / Conseil interne / Formation / Surveillance de la conformité en matière de protection des données
  - Indépendant et non soumis à des directives
  - Avantages : Pas d'obligation de consulter le PFPDT en cas d'analyse d'impact relative à la protection des données

- RGPD : **délégué à la protection des données ->** Non (exception : si l'activité principale consiste à traiter des données à caractère personnel et implique un contrôle systématique)

Recommandation :

La mise en place d'un conseiller à la protection des données est en principe judicieuse. Toutefois, pour les petites entreprises, l'effort ne se justifie guère. Il est également possible de faire appel à un « délégué à la protection des données de l'entreprise ».

14. Protection des données dans le droit du travail

Principe : les données personnelles doivent concerner les **aptitudes** du travailleur ou être nécessaires à l'exécution du contrat de travail !

Bases juridiques :

- Art. 28 CC (protection de la personnalité)
- Art. 328 CO (devoir d'assistance / protection de la personnalité du travailleur)
- Art. 328b CO (avec référence à la loi sur la protection des données) – applicable par analogie aux **candidatures**
- Art. 26 OLT 3 (interdiction d'utiliser des systèmes de surveillance et de contrôle destinés à surveiller le comportement)
- Droit de consultation : art. 23 LPD et art. 15 RGPD
- Une déclaration de protection des données propre au personnel est recommandée
- Surveillance technique sur le lieu de travail (Internet / e-mail / vidéo / contrôle d'accès, etc.)

https://www.seco.admin.ch/seco/fr/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Arbeit/Arbeitsbedingungen/Broschuren/technische-ueberwachung-am-arbeitsplatz.html

15. Mise en œuvre pratique : précautions du site web

- Mettre en ligne une déclaration de protection des données au niveau supérieur
- Case à cocher (unchecked !) pour la déclaration de protection des données dans les boutiques en ligne (lien vers le document)
- Cases à cocher pour la déclaration de consentement lors des inscriptions (« opt-in »)
- E-mail de confirmation d'inscription (« double opt-in »)
- Possibilité de se désinscrire (« opt-out »)
- Les cookies :
  - Suisse : bannière d'information (à cliquer ; pas de consentement nécessaire)
  - UE : bannière de consentement avec déclaration de consentement obligatoire (selon le règlement E-Privacy)
- Enregistrement des inscriptions ou des désinscriptions à des fins de documentation

15. Mise en œuvre pratique : résumé (à faire)

1. Définir les **responsabilités** au sein de l'entreprise ! Qui est responsable de la protection des données ?
2. Vérifier **l'applicabilité du RGPD**
3. **Identification** des fichiers
4. Examiner les **motifs justificatifs** des traitements de données
5. **Documentation :** créer un registre des traitements de données
6. Vérifier les **déclarations de protection des données** par rapport aux nouvelles dispositions de la LPD (ou du RGPD)
7. Identifier les **sous-traitances** et créer des bases contractuelles si nécessaire
8. Identifier les **transferts de données vers l'étranger** et vérifier leur licéité
9. Définir des **processus internes** pour les droits d'information des personnes concernées (demande d'information, notification des violations de la protection des données, analyse d'impact relative à la protection des données personnelles)
10. Prendre des **mesures techniques et organisationnelles** (site web, réseaux sociaux, marketing)
11. Assurer la **sécurité des données** grâce à des mesures techniques et organisationnelles appropriées

15. Mise en œuvre pratique

« Droit à l'oubli »

Source : https://khalawgroup.com/the-right-to-be-forgotten-gdpr/gdpr-right-to-be-forgotten-cartoon/

Instaurer la confiance auprès de la clientèle et du public grâce à la conformité en matière de protection des données

Source : https://khalawgroup.com/the-right-to-be-forgotten-gdpr/gdpr-right-to-be-forgotten-cartoon/

Liens complémentaires

- Préposé fédéral à la protection des données :https://www.edoeb.admin.ch/edoeb/fr/home.html
- Ancienne loi sur la protection des données : https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/fr
- Loi sur la protection des données actuellement en vigueur : https://www.fedlex.admin.ch/eli/cc/2022/491/fr
- Ordonnance révisée sur la protection des données : https://www.fedlex.admin.ch/eli/cc/2022/568/fr
- RGPD de l'UE : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=fr
- Informations actuelles sur le droit de la protection des données : https://datenrecht.ch/

PARTIE 3 : Questions et réponses

Q&R

Questions et réponses

Droit du travail :
La protection des données « en mémoire » : les anciens candidats (dont les dossiers ont déjà été supprimés) peuvent-ils être contactés ultérieurement pour le même poste vacant, de mémoire ?

En principe, la protection des données s'applique à tout « mode de stockage » de données. Dans l'arrêt 4A_125/2020 , le Tribunal fédéral a dû décider si, lors d'une demande de renseignements, les « **informations disponibles sur l'origine des données** » selon l'art. 8, al. 2, let. a [ancienne] LPD pouvaient également inclure **les connaissances qui se trouvent dans la mémoire humaine**. Le Tribunal fédéral a répondu par la négative, ce qui plaide en faveur de l'admissibilité de la prise de contact « de mémoire ».

Droit du travail :
Les questions de santé des employés peuvent-elles être abordées au sein de la direction ?

En principe, non. Seul le **fait** qu'une personne soit malade peut être abordé, mais aucun détail sur la maladie ne peut être discuté tant que l'employé n'a pas donné son accord. La maladie de quelqu'un ne concerne pas non plus la direction.

Questions et réponses

Existe-t-il des critères de distinction entre les obligations liées au traitement des données personnelles qui n'appartiennent pas directement aux personnes ou qui proviennent de l'emploi dans une entreprise et les données de la vie privée ? Par exemple, adresse e-mail privée vs professionnelle ou numéro de téléphone privé vs numéro direct au travail ?

→

Non, toute donnée à caractère personnel relève de la même manière de la protection des données.
Principe : seules les données nécessaires à la finalité du traitement peuvent être traitées (principe de minimisation des données ou Privacy by default).

Échange de données avec les organes fédéraux
Qu'en est-il de l'échange de données personnelles (telles que le numéro de carte maladie, le numéro AI, etc.) avec la SUVA, l'AI, le SAHB et les institutions (maisons de retraite/de soins) ?

→

L'échange de données étant prévu par la loi, les données personnelles peuvent (ou doivent) être transmises à ces organes fédéraux (motif justificatif « loi »).
La LPD s'applique normalement. Des dispositions particulières s'appliquent toutefois aux organes fédéraux dans le chapitre 6 de la LPD (art. 33 et suivants).

Questions et réponses

Droit à la suppression
Qu'en est-il des données à caractère personnel contenues dans une sauvegarde ? Il n'est pas possible de les modifier ou de les supprimer individuellement sans supprimer l'ensemble de la sauvegarde.

→

En principe, l'obligation de suppression s'applique également aux sauvegardes, dans le respect des délais de conservation légaux. Problème : en cas de restauration des données à partir d'une sauvegarde, les données supprimées en réalité dans le système de production redeviendraient productives et devraient être supprimées à nouveau. Si la suppression est déraisonnable ou entraîne des frais disproportionnés, la suppression ne peut à mon avis pas être exigée (privilégier les « vraies » sauvegardes). Principe : **Privacy by Design** (prendre en compte les processus de suppression dans l'architecture informatique), c'est-à-dire procéder de manière à ce que la suppression soit possible.

Droit du travail
– Droit d'information de l'employé ?
– Déclaration de protection des données pour les collaborateurs ?

→

– Droit d'accès :
L'employé a un droit d'accès au dossier personnel (art. 25 LPD).
– Déclaration de protection des données pour les employés : il est recommandé d'établir une DPD séparée pour les coll. et de la publier sur l'Intranet ou de la remettre en annexe au contrat de travail.

Questions et réponses

Sous-traitance
Dans le domaine B2B (fabrication et vente de lentilles de contact individuelles), faut-il signer un « accord de sous-traitance » supplémentaire ?

Oui, mais seulement si les données personnelles du client final qui utilisera les lentilles de contact fabriquées individuellement sont transmises. Les données à caractère personnel n'étant pas nécessaires à la fabrication des lentilles, il convient de renoncer à l'échange de données à caractère personnel.

Pseudonymisation / Sous-traitance / RGPD
À quoi les entreprises suisses doivent-elles faire attention si elles veulent utiliser des données d'appareils, ou des données médicales **pseudonymisées** d'appareils connectés au cloud pour une « maintenance prédictive » active automatisée ou pour le développement de dispositifs qui sont utilisés dans l'UE ?

À quoi les entreprises allemandes doivent-elles faire attention si elles veulent utiliser les données de leurs appareils utilisés en Suisse ?

Dans un premier temps : les données pures de l'appareil et les **données anonymisées** ne posent aucun problème en matière de protection des données. Pour les données **pseudonymisées** , la situation juridique n'est pas claire quant à l'applicabilité du RGPD/de la loi sur la protection des données.
Le responsable (dans l'UE) devrait conclure un **contrat de sous-traitance** avec une entreprise suisse conformément à l'article 28 du RGPD. Dans le cas inverse, même situation de départ, contrat de sous-traitance selon l'art. 9 LPD.

Questions et réponses

Marketing (motifs justificatifs)
Comment la LPD va-t-elle nous influencer au quotidien en ce qui concerne les activités de marketing direct ?

Le marketing direct est autorisé en Suisse tant que les principes de la protection des données (voir diapositive 8) sont respectés, en particulier si le traitement est proportionné, c'est-à-dire que le seuil de l'**atteinte à la personnalité** ne doit pas être dépassé. Le niveau auquel il se situe dépend des cas individuels et de la pratique future des tribunaux.
RGPD : le motif justificatif de « l'intérêt privé prépondérant » doit être rempli (voir diapositive 9)

Sous-traitance
Nous avons conclu un contrat avec notre partenaire logiciel XY pour le traitement des données à caractère personnel. En tant que distributeur d'aides à la rééducation, devons-nous prendre d'autres dispositions ? Envers nos clients directs ? En termes de messagerie (nous travaillons actuellement avec Outlook) ?

Non, un contrat de sous-traitance suffit. Le recours à un logiciel ou à un sous-traitant est autorisé, les clients ne doivent pas en être informés.

L'utilisation d'Outlook ne change rien à la situation de départ en matière de protection des données.

Questions et réponses

Données personnelles sensibles

a) De quoi devons-nous tenir compte en tant qu'importateur et distributeur ?

b) Que faisons-nous des données de patients qui nous sont envoyées sans que nous les ayons demandées, par exemple sur des ordonnances ou par une clinique ? La suppression de l'e-mail suffit-elle ?

→

a) Prendre en compte les principes généraux de protection des données (diapositive 8).

b) Données de patients non demandées : supprimer et informer l'expéditeur de ne pas transmettre. Si la transmission est autorisée, un contrat de sous-traitance devrait en fait être conclu (obligation du point de vue de l'expéditeur).

Délégué à la protection des données / Conseiller à la protection des données

En tant que petite PME, devons-nous désigner ou avoir un délégué à la protection des données ?

→

Non, ce n'est pas prévu par la loi. Néanmoins, la LPD / le RGPD doivent être respectés, ce qui signifie que chaque organisation devrait clarifier sa responsabilité et nommer un responsable de la protection des données **au sein de l'entreprise** qui s'occupe de ce sujet (voir diapositive 28). Examiner si, le cas échéant, la fonction de conseiller à la protection des données (prévue par la loi) a un sens sur une base volontaire.

Questions et réponses

Droit du travail
Besoin d'un modèle de lettre d'employé que les employés peuvent ou doivent signer (ce à quoi il faut faire attention, ce qui est punissable, etc.)

→

Le comportement à adopter en matière de protection des données devrait être abordé dans un règlement interne (p. ex. directive sur l'utilisation de l'informatique). Les instructions sont des ordres unilatéraux donnés par l'employeur. Un modèle doit être élaboré individuellement.

Liste des activités de traitement
Quels registres doivent être tenus (lieux de stockage, données des collaborateurs, etc.) ?

→

Voir diapositives 24/25

Questions et réponses

Droit à la suppression vs obligation de conservation
La suppression des données clients n'est pas facile dans l'ERP, car les factures doivent encore exister dans la comptabilité.

L'obligation de conservation est de 10 ans (cf. art. 958 let. f CO). Ce motif justificatif légal prévaut sur une demande de suppression.

PARTIE 3 : Questions et réponses

Q&R

Merci beaucoup pour votre attention

Coordonnées :

factum advocatur

Urs Freytag, lic. en droit HSG

Teufenerstrasse 3, 9000 St. Gall

Téléphone: 071 421 41 41

Mail: freytag@factum.pro