Formation continue | HEG-Genève

Cours de préparation au Brevet fédéral de Paralegal

Protection des données

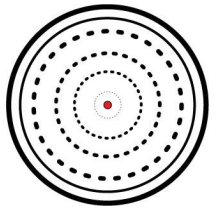
Basile Walder

h e g
Haute école de gestion
Genève

Hes·so GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

Programme

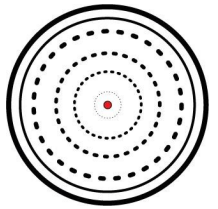
- Introduction générale
- La protection des données en Suisse
- La protection des données dans l'UE
- Exemples de documents et étude de cas



Chapitre 01

Introduction générale

- Qu'est-ce que la protection des données?
- Qu'est-ce qu'une donnée?
- Qu'est-ce qu'une donnée personnelle?
- Quelle est le but de la protection des données?
- Pourquoi existe-t-il un besoin de protection?
- Quelles sont les lois applicables à la protection des données?



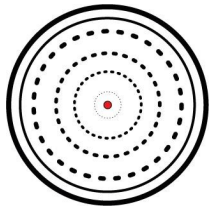
Données personnelles

- Toutes les informations concernant une personne physique identifiée ou identifiable
  - Nom et prénom
  - Adresse e-mail
  - Numéro de téléphone
  - Date de naissance
  - Numéro de candidat
  - Dossier personnel
  - Données sur la santé
  - Etc.

- <u>Exclusion</u>: les données des personnes morales et les données anonymes

Historique/Dates importantes

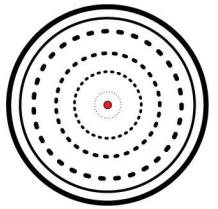
- 19 juin 1992: Adoption de la loi fédérale sur la protection des données (LPD)
- 1995: Adoption de la directive sur la protection des données personnelles 95/46/CE
- 27 avril 2016: Adoption du règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données; RGPD)
- 25 mai 2018: Mise en œuvre du RGPD
- 25 septembre 2020: Adoption de la LPD révisée
- 1er septembre 2023: Mise en œuvre de la LPD révisée



Chapitre 02

La protection des données en Suisse

- Législation applicable:
  - Loi fédérale sur la protection des données (LPD)
  - Ordonnance sur la protection des données (OPDo)
  - Ordonnance sur les certifications en matière de protection des données (OCPD)
  - Dispositions particulières/spécifiques
    - Art. 328b CO
    - Traitement des données par les organes fédéraux
  - Législations cantonales



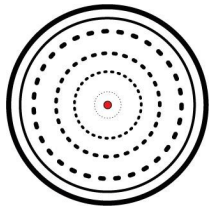
LPD - Champ d'application

Art. 2 LPD

- Matériel:
  - Traitement

    (toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données)
  - Données personnelles

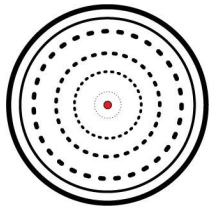
    (toutes les informations concernant une personne physique identifiée ou identifiable)
- Personnel:
  - Personnes privées
  - Organes fédéraux



LPD - Champ d'application

Art. 3 LPD

- Exclusions:
  - Usage exclusivement personnel
  - Chambres fédérales et commissions parlementaires
  - Personnes jouissant d'une immunité de juridiction
  - Procédures (sauf procédures administratives de première instance)
  - Aspects de droit privé relatifs aux registres publics
- Territorial:
  - Etats de fait qui déploient des effets en Suisse, même s'ils se sont produits à l'étranger.



LPD - Acteurs

- Personne concernée

  (la personne physique dont les données personnelles font l'objet d'un traitement)

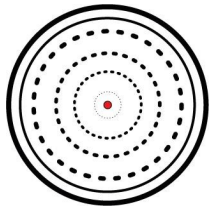
- Responsable du traitement

  (la personne privée ou l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles)

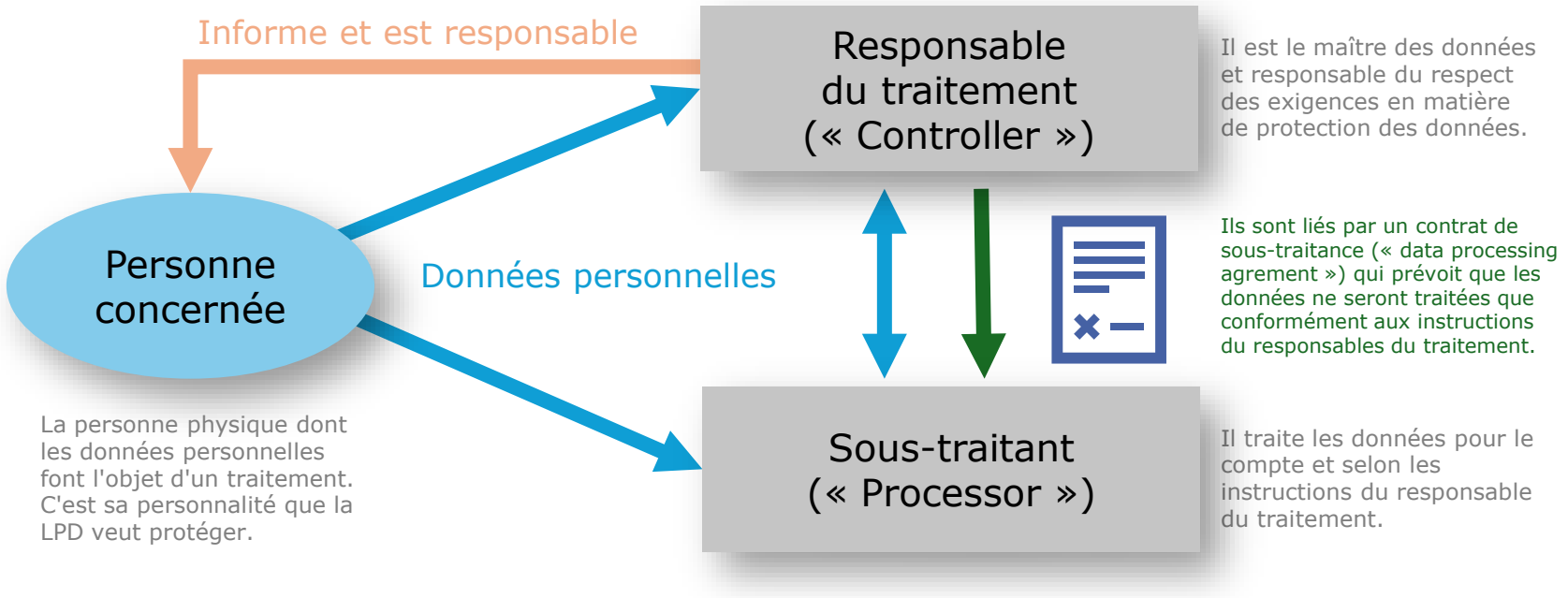
- Sous-traitant

  (la personne privée ou l'organe fédéral qui traite des données personnelles pour le compte du responsable du traitement)

- Préposé fédéral à la protection des données et à la transparence (PFPDT)



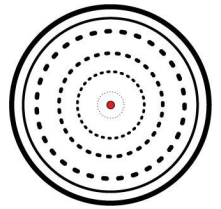
LPD - Acteurs


Informe et est responsable
Responsable du traitement (« Controller »)
Il est le maître des données et responsable du respect des exigences en matière de protection des données.
Personne concernée
Données personnelles
Ils sont liés par un contrat de sous-traitance (« data processing agrement ») qui prévoit que les données ne seront traitées que conformément aux instructions du responsables du traitement.
La personne physique dont les données personnelles font l'objet d'un traitement. C'est sa personnalité que la LPD veut protéger.
Sous-traitant (« Processor »)
Il traite les données pour le compte et selon les instructions du responsable du traitement.

LPD - Autres définitions

Art. 5 LPD

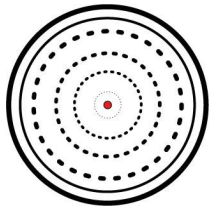
- Données personnelles sensibles (données sensibles):
  - Données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales,
  - Données sur la santé, la sphère intime ou l'origine raciale ou ethnique,
  - Données génétiques,
  - Données biométriques identifiant une personne physique de manière univoque,
  - Données sur des poursuites ou sanctions pénales et administratives,
  - Données sur des mesures d'aide sociale.
- Communication: le fait de transmettre des données personnelles ou de les rendre accessibles.
- Profilage: toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;
- Profilage à risque élevé: tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique;
- Violation de la sécurité des données: toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données;



LPD - Principes

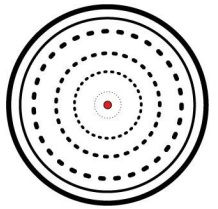
Art. 6-8 LPD

- Licéité
- Transparence
- Bonne foi
- Finalité (ce qui a été communiqué)
- Proportionnalité (par rapport à la finalité)
- Exactitude
- Sécurité



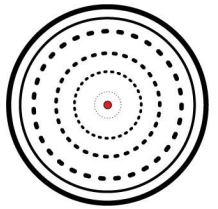
LPD - Principes

- Licéité, transparence et bonne foi
  - Licéité: le traitement de donnée ne doit pas enfreindre une loi qui a pour but direct ou indirect de protéger la personnalité.
    - Exemple: illicite de collecter ou divulguer des données en violation d'un secret, comme le secret bancaire.
  - Transparence: la personne concernée doit pouvoir se rendre compte de l'existence de la collecte, de son moment, du type de données récoltées et des buts → afin qu'elle puisse exercer ses droits le cas échéant.
    - Exemple: une personne filmée doit se rendre compte qu'elle est filmée avant d'entrer dans le champ de vision de la vidéosurveillance.
  - Bonne foi: clause générale
    - Exemple de mauvaise foi: traitement à l'insu de la personne concernée ou contre sa volonté.



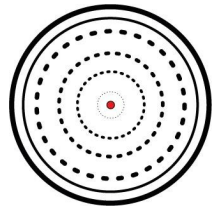
LPD - Principes

- Finalité
  - Détermination du but:
    - Le but doit être déterminé au plus tard au moment de la collecte des données.
    - La collecte de données ne peut être une fin en soi.
    - Le but doit être reconnaissable pour la personne concernée (condition remplie si le traitement est prévu par la loi).
  - Immutabilité du but:
    - Traitement selon le but défini et indiqué lors de la collecte des données.
    - En cas de communication à un tiers, tiers tenu par les buts de la collecte effectuée par le responsable du traitement



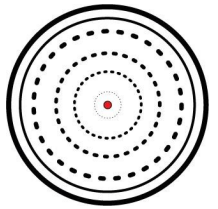
LPD - Principes

- Proportionnalité
  - Aptitude: Le traitement doit être apte à atteindre le but du traitement.
    - Exemple: Vidéosurveillance d'un lieu uniquement si cette mesure est apte à diminuer le vandalisme et identifier les auteurs.
  - Nécessité: L'ampleur du traitement doit être nécessaire pour atteindre le but (quantité de données traitées, durée de conservation, personnes ayant accès à des données).
    - Exemple: Il est uniquement nécessaire pour le bailleur de demander des informations sur la situation financière du locataire avant la conclusion du bail, mais plus après.
  - Proportionnalité au sens étroit: Mise en balance complète entre les intérêts de la personne concernée avec le but visé, y compris en ce qui concerne la durée de conservation des données.
    - Exemple: Il est disproportionné d'installer des caméras à l'extérieur du bâtiment et à l'intérieur (dans ses couloirs) pour prévenir le vandalisme.



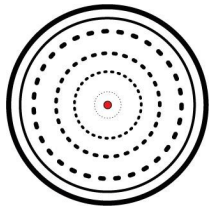
LPD - Principes

- Exactitude
  - Le responsable de traitement doit s'assurer que les données qu'il traite sont exactes.
  - Les données sont exactes si elles reflètent de manière correcte, actuelle et objective les faits ou autres circonstances se rapportant à la personne concernée.
    - L'exactitude est une notion relative car elle dépend de la finalité du traitement / mise à jour potentiellement nécessaire.
  - Si les données sont inexactes: correction ou suppression des données par le responsable du traitement.
  - NB: Le fait de traiter une donnée erronée n'est pas nécessairement une violation du principe d'exactitude. Ce n'est le cas que si le responsable de traitement ne s'assure pas suffisamment de l'exactitude des données.



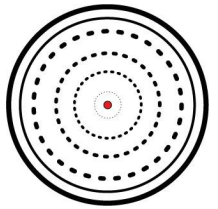
LPD - Principes

- Sécurité
  - Objectif: éviter toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données.
  - Mesures techniques et organisationnelles appropriées par rapport au risque encouru, mais minimum prévu par la loi (cf. art. 1-6 OPDo).
  - Violation si l'incident de sécurité résulte en une atteinte (même potentielle) aux données conservées.
    - Ni la cause (humaine ou technique, fait d'un collaborateur ou du responsable du traitement ou tiers) de l'incident, ni l'existence d'une intention ou négligence de la part du responsable du traitement ne sont déterminants pour l'existence de la violation.



LPD - Principes

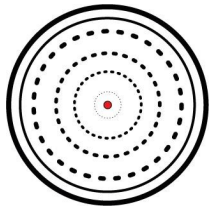
- Protection dès la conception et par défaut
  - Mise en place de mesures organisationnelles et techniques afin que le traitement respecte les principes de la LPD dès sa conception.
    - Exemples:
      - Anonymisation (irréversible) des données;
      - Pseudonymisation des données;
      - Cryptage ou chiffrement des données.
  - Protection par défaut: Le traitement doit être paramétré de manière à ce qu'il soit le moins invasif possible pour la personne concernée.



LPD - Obligations du responsable de traitement

Art. 12 LPD

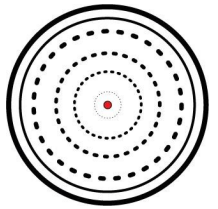
- Registre des activités de traitement
  - Pour les responsables de traitement et les sous-contractants.
  - Contenu minimum.
  - Exception pour les entreprises de moins de 250 collaborateurs, pour autant que le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées



LPD - Obligations du responsable de traitement

Art. 19-21 LPD

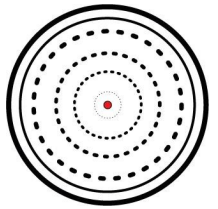
- Devoir d'informer lors de la collecte de données personnelles
  - Contenu:
    - Informations nécessaires pour faire valoir ses droits
    - Informations nécessaires pour que la transparence des traitements soit garantie
    - Identité et coordonnées du responsable du traitement
    - Finalité du traitement
    - Destinataires ou catégories de destinataires auxquels des données personnelles sont transmises
    - En cas de collecte indirecte, catégories de données traitées
    - En cas de communication à l'étranger, nom de l'État ou de l'organisme international auquel elles sont communiquées et, le cas échéant, les garanties et exceptions applicables
  - Exceptions
  - Décision individuelle automatisée (information et revue par une personne physique)



LPD - Obligations du responsable de traitement

Art. 9 LPD

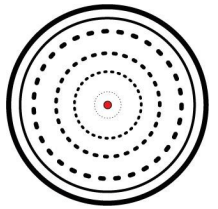
- Sous-traitance
  - Conditions:
    - Un contrat ou la loi le prévoit;
    - Les traitements effectués sont ceux que le responsable de traitement serait en droit d'effectuer lui-même; et
    - Aucune obligation légale ou contractuelle de garder le secret ne l'interdit.
  - Responsable du traitement doit s'assurer que le sous-traitant assure la sécurité des données.



LPD - Obligations du responsable de traitement

Art. 22-23 LPD

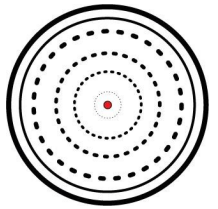
- Analyse d'impact
  - Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.
  - Exceptions: Traitement prévu par la loi, produit ou service certifié, ou code de conduite.
  - Contenu: Description du traitement envisagé, évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, et mesures prévues pour protéger sa personnalité et ses droits fondamentaux.
  - Si l'analyse d'impact révèle un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée malgré les mesures prévues, consultation du PFPDT (exception: conseiller à la protection des données).



LPD - Obligations du responsable de traitement

Art. 24 LPD

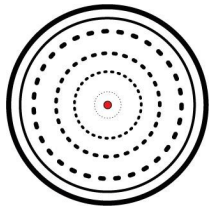
- Annonce des violations de la sécurité des données
  - Cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.
  - Annonce au PFPDT dans les meilleurs délais, et à la personne concernée si nécessaire à sa protection ou exigé par le PFPDT.
  - Contenu: Nature de la violation de la sécurité des données, ses conséquences et les mesures prises ou envisagées.
  - Obligation similaire du sous-traitant envers le responsable du traitement.



LPD -Obligations du responsable de traitement

Art. 16-18 LPD

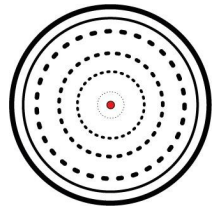
- Communications des données à l'étranger
  - Communication possible si:
    - Etat ou organisme international garantit un niveau de protection adéquat (cf. Annexe 1 OPDo)
    - Niveau de protection approprié garanti par d'autres mesures
    - Dérogations applicables
  - Publication de données personnelles afin d'informer le public n'est pas assimilée à une communication à l'étranger, même si les données peuvent être consultées depuis l'étranger.



LPD - Obligations du responsable de traitement

Art. 14-15 LPD

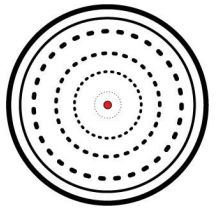
- Siège ou domicile à l'étranger
  - Obligation de désigner un représentant en Suisse si:
    - Traitement de données personnelles concernant des personnes en Suisse
    - Traitement en rapport avec l'offre de biens ou de services ou le suivi du comportement de personnes en Suisse
    - Traitement à grande échelle
    - Traitement régulier
    - Traitement présente un risque élevé pour la personnalité des personnes concernées
  - Point de contact pour les personnes concernées et le PFPDT.
  - Publication du nom et de l'adresse du représentant par le responsable du traitement.



LPD - Droits de la personne concernée

Art. 25-27 LPD

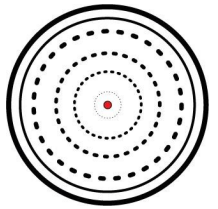
- Droit d'accès
  - Droit de demander au responsable du traitement si des données personnelles le concernant sont traitées.
  - Y compris en cas de traitement par un sous-traitant.
  - Contenu: Informations nécessaires pour faire valoir ses droits et pour que la transparence du traitement soit garantie.
  - En règle générale, procédure gratuite et délai de 30 jours pour y donner suite.
  - Restrictions



LPD - Droits de la personne concernée

Art. 28-29 LPD

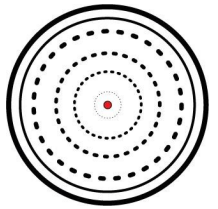
- Droit à la remise ou à la transmission de données personnelles
  - Conditions:
    - le responsable du traitement traite les données personnelles de manière automatisée; et
    - les données personnelles sont traitées avec le consentement de la personne concernée ou en relation directe avec la conclusion ou l'exécution d'un contrat entre elle et le responsable du traitement.
  - Remise sous un format électronique couramment utilisé, directement à la personne concernée ou à un autre responsable de traitement.
  - En règle générale, procédure gratuite.
  - Restrictions.



LPD - Atteintes à la personnalité

Art. 30-31 LPD

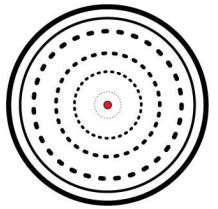
- Uniquement pour les traitements par des personnes privées
- Le traitement des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées.
- Exemples:
  - traiter des données personnelles en violation des principes de la LPD;
  - traiter des données personnelles contre la manifestation expresse de la volonté de la personne concernée;
  - communiquer à des tiers des données sensibles.
- Une atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la personne concernée, par un intérêt privé ou public prépondérant, ou par la loi.
- En principe, pas d'atteinte lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée expressément au traitement.



LPD - Atteintes à la personnalité

Art. 32 LPD

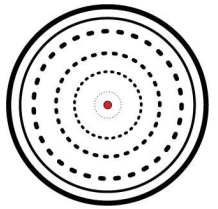
- Prétentions:
  - Rectification des données personnelles inexactes
  - interdiction d'un traitement déterminé
  - interdiction d'une communication déterminée de données personnelles à des tiers
  - effacement ou la destruction de données personnelles
  - Mention du caractère litigieux de l'exactitude ou l'inexactitude d'une donnée personnelle
  - Communications à des tiers ou publications



LPD - Organes fédéraux

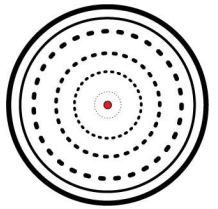
Art. 33-42 LPD

- Définition: Autorité fédérale, service fédéral ou personne chargée d'une tâche publique de la Confédération.
- Traitement (et communications) de données personnelles uniquement s'il existe une base légale (dans une loi au sens formel pour certains cas).
- Déclaration du registre d'activités de traitements au PFPDT (Art. 12 al. 4 LPD).
- Obligation de nommer un conseiller à la protection des données (Art. 25 OPDo).



LPD - Organes fédéraux

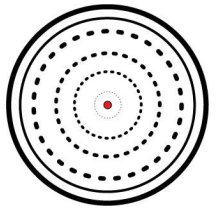
- Prétentions
  - Conditions: Intérêt digne de protection.
  - Mesures:
    - s'abstenir de procéder à un traitement illicite
    - supprimer les effets d'un traitement illicite
    - constater le caractère illicite du traitement
    - rectifier les données personnelles, les effacer ou les détruire
    - publier ou communiquer à des tiers sa décision
  - Procédure régie par la Loi fédérale sur la procédure administrative (PA)



LPD - PFPDT

Art. 49-53 LPD

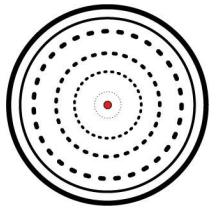
- Enquête: Si des indices suffisants font penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données
- Pouvoir d'ordonner:
  - l'accès à tous les renseignements, documents, registres des activités de traitement et données personnelles nécessaires pour l'enquête
  - l'accès aux locaux et aux installations
  - l'audition de témoins
  - des expertises
- Si des dispositions de protection des données sont violées, le PFPDT peut ordonner la modification, la suspension ou la cessation de tout ou partie du traitement ainsi que l'effacement ou la destruction de tout ou partie des données personnelles, ou suspendre ou interdire la communication de données personnelles à l'étranger.
- Procédure régie par la Loi fédérale sur la procédure administrative (PA)



LPD - Dispositions pénales

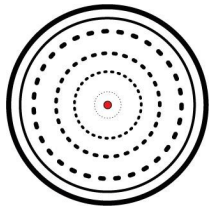
Art. 60-66 LPD

- En cas de violation des obligations d'informer, de renseigner et de collaborer, des devoirs de diligence ou du devoir de discrétion, ou en cas d'insoumission à une décision du PFPDT.
- Uniquement en cas d'intention.
- Peine maximale: amende de CHF 250'000.- pour les personnes concernées (i.e. pas de condamnation de l'entreprise, sauf exception).
- Poursuite et jugements par les autorités cantonales.



Législations cantonales

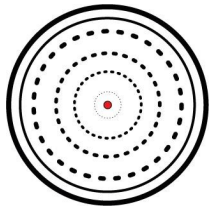
- GE – Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD)
- VD – Loi sur la protection des données personnelles (LPrD)
- FR – Loi sur la protection des données (LPrD)
- VS – Loi sur l'information du public, la protection des données et l'archivage (LIPDA)
- NE et JU – Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE)
- Etc.



Chapitre 03

La protection des données dans l'UE

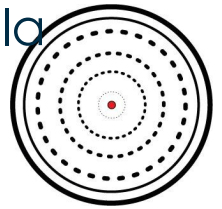
Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données; RGPD)



RGPD - Champ d'application

Art. 2-3 RGPD

- Matériel:
  - Traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.
  - Exception notamment pour les traitements par une personne physique dans le cadre d'une activité strictement personnelle ou domestique.
- Territorial:
  - Traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.
  - Traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'Union, ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

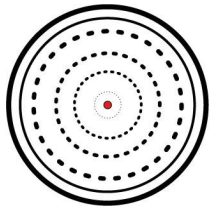


RGPD - Principes

Art. 5 RGPD

Les données à caractère personnel doivent être:

- traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);
- collectées pour des finalités déterminées, explicites et légitimes (limitation des finalités);
- adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);
- exactes et, si nécessaire, tenues à jour (exactitude);
- conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (limitation de la conservation);
- traitées de façon à garantir une sécurité appropriée des données à caractère personnel, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

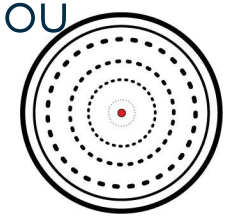


RGPD - Principes

Art. 6 RGPD

Le traitement n'est licite que si au moins une des conditions suivantes est remplie:

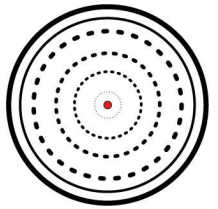
- la personne concernée a consenti au traitement de ses données à caractère personnel;
- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles;
- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée.



RGPD - Principes

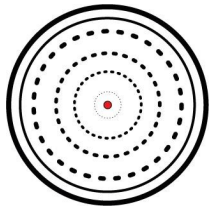
Art. 9 RGPD

Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits, sauf exceptions.



RGPD – Responsable du traitement

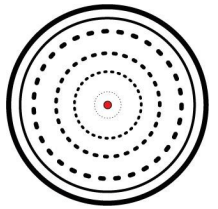
- Informations à fournir lorsque des données à caractère personnel sont collectées (Art. 13-14 RGPD)
- Protection des données dès la conception et protection des données par défaut (Art. 25 RGPD)
- Registre des activités de traitement (Art. 30 RGPD)
- Sécurité du traitement (Art. 32 RGPD)
- Notification à l'autorité de contrôle et à la personne concernée d'une violation de données à caractère personnel (Art. 33-34 RGPD)
- Analyse d'impact (Art. 35-36 RGPD)
- Désignation d'un représentant dans l'Union européenne (Art. 27 RGPD)



RGPD – Sous-traitant

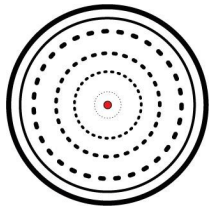
Art. 28-29 RGPD

- Nécessité d'un contrat ou un autre acte juridique pour le traitement des données par le sous-traitant qui doit contenir un contenu minimum (notamment, l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, les obligations et les droits du responsable du traitement).
- Traitement uniquement sur instruction du responsable de traitement.



RGPD – Personnes concernées

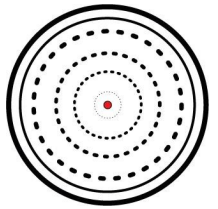
- Droit d'accès (Art. 15 RGPD)
- Droit de rectification (Art. 16 RGPD)
- Droit à l'effacement (Art. 17 RGPD)
- Droit à la limitation du traitement (Art. 18 RGPD)
- Droit à la portabilité des données (Art. 20 RGPD)
- Droits en cas de décision individuelle automatisée (Art. 22 RGPD)
- Droit d'introduire une réclamation auprès d'une autorité de contrôle (Art. 77 RGPD)



RGPD - Sanctions

Art. 83 RGPD

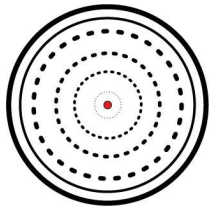
Les violations du RGPD et le non-respect d'une injonction émise par l'autorité de contrôle peuvent faire l'objet d'amendes administratives pouvant s'élever jusqu'à EUR 20’000’000.- ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.



RGPD vs. LPD

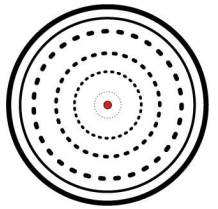
Récapitulatif

(voir document comparatif)



Autres législations européennes

- Règlement européen concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données)
- Règlement européen portant sur la gouvernance européenne des données (règlement sur la gouvernance des données)
- Règlement européen établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle)
- Etc.



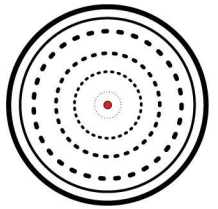
Chapitre 04

Exemples de documents

- Politique de confidentialité:

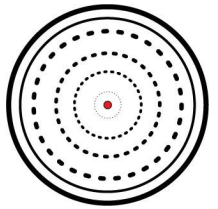
https://www.vischer.com/fr/protection-des-donnees/

https://dsat.ch/download/3/dsat/404/modele-de-declaration-de-protection-des-donnees-general-version-5-4-2022-fr.docx



Exemples de documents

- Accord de sous-traitance



Exemples de documents

- La LPD sur une page

nLPD – Ce qu'il faut faire.

Pour les PME

Mis en oeuvre : ☑

Nouveau dès 1.9.2023

Dix commandements pour le traitement des données selon la LPD[1]

1. Nous **disons** aux personnes ce que nous faisons de leurs données et pourquoi.
2. Nous **nous y tenons** et n'utilisons pas les données à d'autres fins.
3. Nous pratiquons la **minimisation des données** et le "besoin de savoir".
4. Nous **supprimons** les données dès que nous n'en avons plus besoin.
5. Nous permettons aux personnes de dire "**non**" au traitement.
6. Nous ne faisons que ce que nous trouverions **acceptable** pour nous-mêmes.
7. Nous vérifions que nos données ne contiennent pas **d'erreurs** ou de lacunes problématiques.
8. Nous ne transmettons pas de **données sensibles**[2] à des tiers.
9. Nous prenons des mesures pour garantir la **sécurité** des données chez nous.
10. Nous obtenons des données **légalement** et à partir de sources légales.

Exceptions (uniquement) possibles en cas d'intérêts légitimes prépondérants. Nous concevons chaque traitement selon ces principes !

Politique de confidentialité

Toute collecte planifiée de données qui n'est pas exigée par la loi doit être mentionnée dans la pol. de confidentialité.

Nous renvoyons les personnes à la politique (dans les CG, les apps, les formulaires, etc.). Elle se trouve sur notre site.

Contenu obligatoire :

Qui nous sommes (avec les coordonnées), les données collectées et les finalités, les destinataires des données (noms non requis) et les pays ou régions concernés (y.c. les bases juridiques invoquées[3]).

Registre des traitements

Nous tenons un registre de nos traitements de données (p. ex. gestion des données clients, comptabilité, gestion RH, boutique en ligne). Son contenu est conforme à l'art. 12 nLPD, e.a. les finalités du traitement, les catégories de personnes, de données et de destinataires et la période de conservation.[4]

Cette **obligation ne s'applique que** si nous avons 250+ employés (effectif) ou si nous traitons des données sensibles à grande échelle ou si nous pratiquons le profilage à risque élevé.

Sous-traitants sous contrôle

Si nous confions le traitement de nos données à un prestataire IT ou à une autre personne, nous concluons un "DPA", c.-à-d. un **contrat** qui nous permet de gérer et contrôler l'entreprise et d'approuver (ou de s'opposer) au préalable au recours à des tiers.[5] Il définit aussi les **mesures de sécurité** ("TOMS"). Nous les vérifions (y.c., si nécessaire, les rapports d'audit). Un DPA selon l'art. 28 RGPD est suffisant s'il renvoie aussi à la LPD. Le sous-traitant ne peut faire que ce que nous sommes autorisés à faire (p. ex. généralement pas de traitement à des fins propres). Nous vérifions la conformité des DPA actuels/nouveaux.

Lorsque les données vont à l'étranger

Sans problème : EEE, UK, pays adéquats[6]

Tous les **autres pays** autorisés si e.a. :

- Transfert nécessaire à l'exécution d'un contrat avec ou dans l'intérêt de la personne concernée
- Renonciation explicite à la protection à l'étranger
- Conclusion des "clauses contractuelles types" de l'UE[6] avec adaptation CH et aucune raison de penser que l'accès aux données par des autorités sera problématique (effectuer un TIA[6,7]).

Nous vérifions nos contrats à cet égard !

Nous garantissons les droits des personnes concernées

Nous **identifions** correctement la personne au préalable. Nous fournissons à une personne **ses propres données personnelles** (pas de documents) et, sur demande, certaines autres informations (en général gratuitement dans un délai de 30 jours). Nous évitons de donner l'impression que nous avons fourni toutes les données (car les renseignements faux ou incomplets sont punissables). Notre première réponse peut se limiter aux données habituellement recherchées par les personnes.

La personne doit nous aider à identifier d'autres données. Les demandes non motivées par la protection des données ne sont pas protégées. Nous protégeons les données des tiers et nos propres secrets d'affaires.

Toute personne peut demander la **rectification** de ses données. Si l'exactitude est contestée, nous le signalons.

Toute personne peut demander la **suppression** de ses données ou nous demander d'arrêter ou de modifier notre traitement. Nous pouvons continuer si nous avons une raison prépondérante de le faire.

Si un **ordinateur** prend des décisions discrétionnaires ayant d'importantes conséquences négatives, nous en informons les personnes concernées et leur proposons une audition humaine.

Dans certains cas, nous devons **remettre** aux personnes les données personnelles qu'elles nous ont communiquées, en vue de leur réutilisation.

Nous veillons à ce que ces droits soient respectés !

Analyse d'impact relative à la protection des données (AIPD)

Pour les projets pouvant présenter un **risque** pour les personnes en termes de traitement des données, nous procédons à une AIPD. Nous y décrivons le projet et les mesures de protection, et vérifions s'il reste malgré tout des risques élevés en termes de **conséquences négatives** indésirables pour elles (le cas échéant : demander conseil). Nous conservons les AIPD.

Privacy by default

Lorsque nous avons des **paramètres** de confidentialité sur des sites web, apps, etc., ils sont **prédéfinis** au **minimum**. Nos développeurs y veillent.

Les données sont sécurisées, sinon nous le signalons

Mesures techniques : Accès uniquement selon le principe du "besoin de savoir" et avec un compte personnel, authentification multifacteur en cas d'accès externe, pistes d'audit (év. obligatoires pour les données sensibles[2], à conserver pendant 1 an), pseudonymisation, pare-feu, logiciel anti-malware, sauvegardes (également hors ligne).

Mesures organisationnelles : Directives (p. ex. utiliser cette page), formations, examen des "logs", s'il y a beaucoup de données sensibles[2], vérifier vos mesures et créer une politique de traitement.

Devoir d'annonce : Si la confidentialité, l'intégrité ou la disponibilité des données personnelles est violée et qu'il existe un risque élevé de conséquences négatives pour les personnes concernées (pas simplement une nuisance), le cas doit être annoncé au PFPDT (formulaire sur https://edoeb.admin.ch) et être documenté pendant 2 ans ; si les personnes concernées ne peuvent pas se protéger elles-mêmes des conséquences, le cas doit aussi leur être annoncé.

Chacun est coresponsable de la sécurité !

Petit secret professionnel

Nous gardons secrètes les données personnelles qui nous sont **confiées** et qui sont nécessaires à l'exercice de notre profession, ou nous indiquons clairement au préalable que nous ne les garderons pas secrètes.

Nous ne nous basons pas sur le consentement

En principe, nous ne nous basons pas sur le consentement. Si c'est le cas, il doit être **volontaire et éclairé**. En cas de données sensibles[2] et de profilage à risque élevé, il doit être explicite.

Nous avons quelqu'un qui sait ce qu'il faut faire quand…

… une personne veut consulter/obtenir ses données ou les faire effacer ou rectifier ou a une autre préoccupation concernant la protection de ses données :

… nous avons un projet nouveau ou modifié qui concerne également des données de personnes et qui doit donc faire l'objet d'une vérification de la protection des données (év. avec AIPD) :

… des données personnelles sont perdues, tombent entre de mauvaises mains, ont été manipulées, que cela ait pu se produire ou qu'il y ait d'autres problèmes de sécurité :

Chacun signale immédiatement de tels incidents à cette personne !

Questions ? (FAQ : https://bit.ly/3EOeiBL et plus : https://bit.ly/2bCmuAO)

Interne :

Externe :

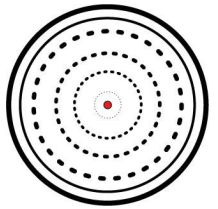
[1] nLPD : https://fedlex.admin.ch/eli/fga/2020/1998/fr
[2] Données personnelles sensibles : Art. 5 let. c nLPD
[3] Voir modèle de pol. de confidentialité : https://dsat.ch
[4] Modèles : https://dsat.ch, https://bit.ly/3qrpOib (DE)
[5] Voir Annexe 1 de l'OPDo (https://bit.ly/3VRjHKS)
[6] Voir FAQ (avec sources) : https://bit.ly/3MBiITE (EN)
[7] Voir TIA : https://bit.ly/3L8mxYO (avec réf. au FAQ)

Auteur : David Rosenthal, drosenthal@vischer.com Trad. : Samira Studer et Julie Nikles Tous droits réservés. Peut être librement diffusé/utilisé sans modification. Il s'agit d'informations, pas de conseils juridiques.

VISCHER

Exemples de documents

- Autres:
    - Registre des activités de traitement
    - Analyse d'impact
    - Règlement sur la protection des données
    - *Data Processing Agreement* (DPA)
    - Etc.



Exemples de documents

- VISCHER Privacy Score

https://privacyscore.ch/en/

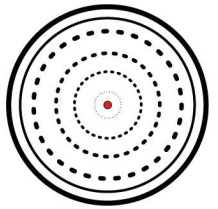
Etude de cas

Le représentant d'une entreprise vous consulte pour s'assurer que les activités de son entreprise sont conformes à la protection des données.

Quelles sont les démarches à entreprendre?

Quels sont les documents minimaux à mettre en place?

Quels sont les points d'attention?



Etude de cas

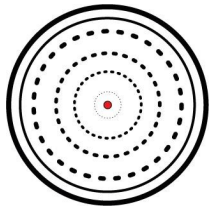
Le représentant d'une entreprise vous consulte suite à un problème informatique ayant empêché l'entreprise d'accéder à ses données et aux données de ses clients pendant une période de 24h.

Quelles sont les démarches à entreprendre?

La situation est-elle différente si le problème informatique a permis à des tiers d'obtenir des données bancaires de clients?

Quel est le risque pour l'entreprise et son représentant:

- Sous l'angle de la LPD?
- Sous l'angle du RGPD?

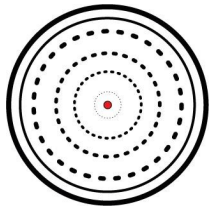


Etude de cas

Le représentant d'une entreprise vous consulte suite à la réception d'une demande d'une personne concernée visant à (i) s'informer sur le traitement des données effectué, et (ii) effacer l'intégralité de ses données personnelles.

Quelles sont les démarches à entreprendre?

Est-il possible de s'opposer à ces demandes?



Merci de votre attention !

h e g

Haute école de gestion
Genève

Hes·so GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale