La modification de la Loi sur la protection des données (LPD)

En général et les impacts en matière de ressources humaines

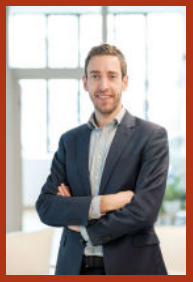
David Raedler

7 mars 2023

1

Les données personnelles du conférencier

- David Raedler
  - Doctorat en droit (enquêtes internes)
  - Spécialiste FSA en droit du travail et protection des don
  - Associé à l'Etude HDC
  - Député dans le Canton de Vaud
  - Chargé de cours à l'Université de Lausanne



2

Un sujet en pleine actualité…

3

…, *a fortiori* dans un contexte toujours plus numérique!

4

Programme

- Cadre juridique
- Les notions et grands principes fondamentaux
- Les changements liés à la nLPD sous l'angle RH
- Comment mettre en œuvre et mettre à jour ses processus internes ?

5

LE CADRE JURIDIQUE

6

Sphère privée et protection des données

- Article 8 § 1 CEDH
  - Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
- Article 13 al. 2 Constitution fédérale
  - Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent.
- Les normes de protection des données visent à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données.

7

Le droit suisse

- Niveau fédéral
  - Loi fédérale sur la protection des données (LPD)
  - Ordonnances
  - Autres textes légaux prenant en compte la protection des données
- Niveau cantonal
  - 25 Lois cantonales sur la protection des données

8

Lois cantonales en particulier

- Exemples
  - Genève: **LIPAD** (Loi sur l'information du public, l'accès aux documents et la protection des données personnelles du 5 octobre 2001, RS/GE A 2 08)
  - Vaud: **LPrD** (Loi sur la protection des données personnelles du 11 septembre 2007, RS/VD 172.65)
  - Fribourg: **LPrD** (Loi sur la protection des données du 25 novembre 1994, RS/FR 17.1)
  - Valais: **LIPDA** (Loi sur l'information, la protection des données et l'archivage)
  - Neuchâtel et Jura: **CPDT-JUNE** (Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel des 8 et 9 mai 2012 , RS/NE 150.30)

Evolution du droit suisse

- Révision de la LPD
  - Projet lancé en 2010
  - Avant-projet présenté en décembre 2016
  - Projet et message du Conseil fédéral présentés le 15 septembre 2017
  - Adoption le 24 septembre 2020!
  - Entrée en vigueur le 1er septembre 2023
  - Buts:
    - Se rapprocher du droit européen
    - Renforcer les droits des personnes concernées
    - Renforcer les pouvoirs d'enquête du Préposé

Droit européen

- Le RGPD!
  - Entrée en vigueur le 25 mai 2018
- Caractéristiques
  - Texte très détaillé sur la protection des données (173 considérants, 99 articles, 88 pages)
  - Directement applicable à tous les Etats membres de l'UE
  - Régime légal très strict
    - Des obligations strictes pour le responsable du traitement
    - Des droits renforcés pour la personne concernée
    - Des amendes administratives importantes (jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent)

11

Droit européen en Suisse

- Art. 3 RGPD (champ d'application territorial)
  - Extension du champ d'application
    - Activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'UE, que le traitement ait lieu ou non dans l'UE.
    - Activités d'un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'UE, pour les données de personnes concernées qui se trouvent sur le territoire de l'UE s'il leur offre des biens ou des services; ou suit leur comportement dans l'UE (p.ex par des cookies)
  - Conséquence: effet «direct» du RGPD sur plusieurs entreprises en Suisse!
- Lignes directrices EDPB 3/2018
- Et en RH?

12

TERMES ET NOTIONS

13

Données personnelles

- Sont des données personnelles, toutes les informations qui se rapportent à une personne identifiée ou identifiable (art. 3 LPD; art. 5 fLPD; art. 4 RGPD).
- En droit suisse, une personne peut être une personne physique («être humain») ou une personne morale («entreprise»).
  - La fLPD s'appliquera uniquement aux personnes physiques
  - Le RGPD ne protège pas les données des personnes morales
- Exemples
  - Nom
  - Numéro de téléphone
  - Adresse IP
  - Adresse électronique
  - Adresse postale
  - Numéro AVS
  - Numéro d'immatriculation
  - Numéro de compte bancaire
  - Photos
  - Vidéosurveillance

14

Données personnelles sensibles

- Catégorie spéciale: les données sensibles
- Concept se retrouvant dans les différents textes applicables
  - Art. 3 let. c LPD et art. 5 let. c fLPD
  - Art. 9 RGPD («catégories particulières de données à caractère personnel»)
- Selon la LPD, sont des données sensibles, les données personnelles sur :
  - les opinions ou activités religieuses, philosophiques, politiques ou syndicales,
  - la santé, la sphère intime ou l'appartenance à une race,
  - des mesures d'aide sociale,
  - des poursuites ou sanctions pénales et administratives.
- Selon le RGPD:
  - données sur l'origine raciale ou ethnique,
  - les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale,
  - les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé et les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

15

Le profilage

- Notion générale
  - L'évaluation de certaines caractéristiques d'une personne sur la base de données personnelles traitées de manière automatisée afin notamment d'analyser ou de prédire son rendement au travail, sa situation économique, sa santé, son comportement, ses préférences, sa localisation ou ses déplacements (art. 4 al. 4 RGPD)
  - Proche du profil de la personnalité de l'art .3 let. d LPD
- Le profilage dans la fLPD: une distinction en «*Swiss finish*»
  - 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 (art. 5 let. f fLPD)
  - 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.

16

Le traitement

- Est un traitement toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés (art. 3 LPD; art. 5 fLPD; art. 4 RGPD)
  - Très large
  - «Tout» est un traitement

17

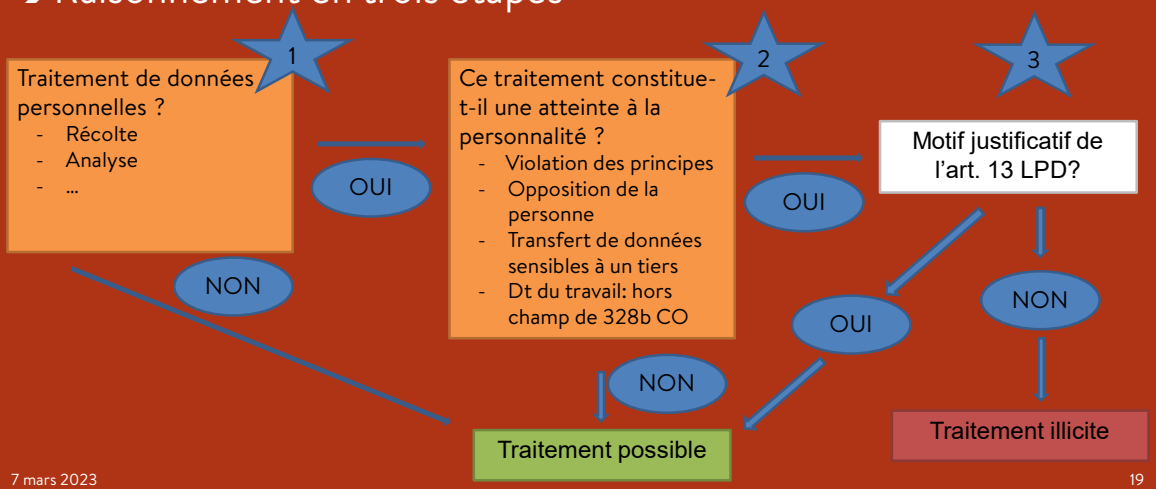
Les principes fondamentaux

- Art. 4, 5 et 7 LPD / Art. 6, 7 et 8 fLPD
- Art. 5 RGPD
- Six principes fondamentaux
  - Bonne foi
  - Proportionnalité
  - Reconnaissabilité (LPD) / Information (RGPD / P-LPD)
  - Exactitude
  - Finalité
  - Sécurité

18

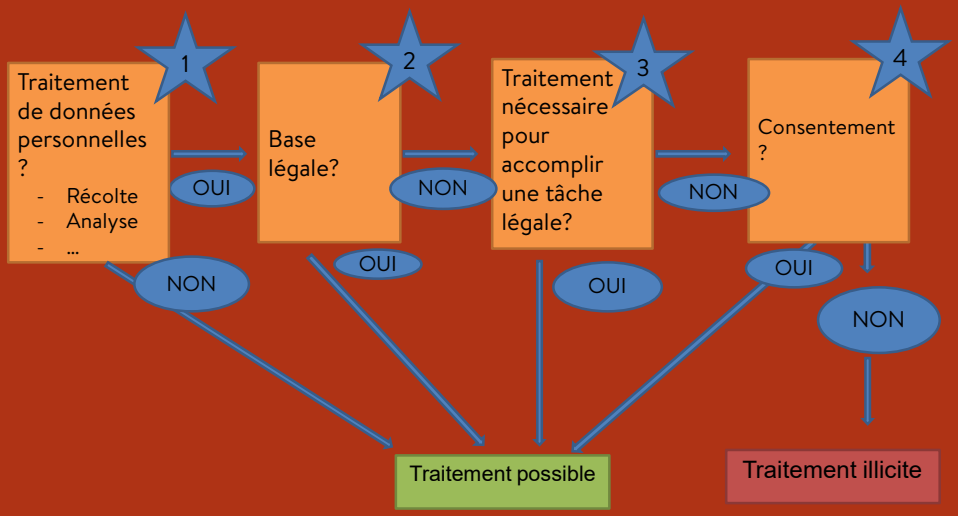
La légalité du traitement en droit suisse

➔Raisonnement en trois étapes



19

Raisonnement en droit cantonal



20

LES CHANGEMENTS DANS LA NLPD

Les obligations aujourd'hui pour les personnes privées

- Respecter les principes de la LPD
- Tenir et déclarer les «fichiers» (art. 11a LPD)
  - Obligation
    - Si des données sensibles ou des profils de la personnalité sont régulièrement traités
    - Si des données personnelles sont régulièrement communiquées à des tiers
  - Exceptions, notamment
    - Si le traitement est prévu par la loi
    - Si qualification par le Conseil fédéral comme n'étant pas risqué
    - Si un DPO a été nommé

Les obligations supplémentaires dans la nLPD

- Protection des données dès la conception et par défaut (art. 7 nLPD)
- Registre des activités de traitement (art. 12 nLPD; art. 30 RGPD)
- Devoir d'informer très marqué (art. 19-20 nLPD; art. 12 ss RGPD)
- Devoir d'informer additionnel en cas de décisions individuelles automatisées (art. 21 nLPD; art. 21 RGPD)
- Analyse d'impact préalable (art. 22 nLPD; art. 35 RGPD)
- Consultation préalable (art. 23 nLPD; art. 36 RGPD)
- Annonce de failles de sécurité (art. 24 nLPD; art. 33 et 34 RGPD)
- Mentions obligatoires dans le contrat de sous-traitance (art. 28 RGPD, pas à art. 9 nLPD)
- Obligation de nommer un DPO (art. 37 ss RGPD)
- Obligation de nommer un représentant dans l'UE (art. 27 RGPD) ou en Suisse (art. 14 ss nLPD)

Obligations en droit cantonal

- Varient selon le droit cantonal applicable
- Mais dans l'ensemble, tendent à ressembler à celle valant en droit fédéral pour les organes fédéraux
  - Mais: compétence des autorités de protection des données cantonales.

Protection des données dès la conception et par défaut

- Art. 7 nLPD
  - Mise en place des mesures permettant de respecter les principes, ceci dès la conception
  - Mesures techniques et organisationnelles appropriées
  - Préréglages par défaut

25

Le registre des activités de traitement

- Art. 30 RGPD et art. 12 fLPD
- Tous les responsables du traitement et tous les sous-traitants doivent maintenir un tel registre
- Modèles établis par les différentes autorités nationales
  - A choisir: IOC (Royaume-Uni), CNIL ou autorité belge

26

Le registre des activités de traitement

- Qu'y mettre?
  - Doit contenir au moins:
    - l'identité du responsable du traitement
    - la finalité du traitement
    - une description des catégories de personnes concernées et des catégories de données personnelles traitées
    - Les catégories de destinataires
    - dans la mesure du possible, le délai de conservation des données personnelles ou les critères pour déterminer la durée de conservation;
    - dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données selon l'art. 8;
    - en cas de communication de données personnelles à l'étranger, le nom de l'Etat concerné et les garanties prévues à l'art. 16, al. 2.

27

Le registre des activités de traitement

- Comment faire?
  - Procéder à un audit interne pour comprendre quels sont les traitements effectués
  - Identifier, lors de l'audit, les autres points à intégrer au registre
  - Faire compléter le registre par les personnes compétentes, selon un document précis
  - Vérifier le document
  - Conserver le registre à l'interne
  - Tenir le registre à jour

28

Le registre des activités de traitement

- Exemple pratique
  - Exemple CNIL:
    - https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf
  - Exemple Belgique:
    - https://www.autoriteprotectiondonnees.be/publications/modele-registre-des-activites-de-traitement-detaille.xlsx

Le devoir d'informer

- Obligation générale, sauf si (art. 20 nLPD):
  - La personne dispose déjà des informations
  - Traitements prévus par la loi
  - Obligation légale de garder le secret (*pour personnes privées*)
  - Exception pour les médias (*renvoi à l'art. 27 nLPD*)

Le devoir d'informer

- Contenu de la notice d'information, au moins:
  - l'identité et les coordonnées du responsable du traitement
  - la finalité du traitement
  - le cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises
  - si les données ne sont pas collectées auprès de la personne concernée, les catégories de données traitées.

Le devoir d'informer

- Forme du devoir d'informer
  - Notice d'information
  - Communication de la notice
    - Site Internet
    - Formulaires
    - Règlement d'entreprise
    - Autres
  - «Facile et complet»
- Exemples pratiques:
  - https://www.easyjet.com/FR/policy/privacy-promise
  - https://www.nestle.ch/fr/info/privacy

Le devoir d'informer en cas de décisions individuelles automatisées

- Art. 21 nLPD
- Notion de «décision individuelle automatisée»
  - Décision (*effets juridiques ou impact significatif*)
  - Algorithme
- Droits de la personne concernée
  - Information spécifique
  - Droit à ce que la décision soit revue par une personne physique
- Exception
  - Conclusion d'un contrat *et* demande satisfaite
  - Consentement exprès

L'analyse d'impact

- Art. 22 nLPD
- Notion d'analyse d'impact
- Condition: risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée
  - Recours à de nouvelles technologies
  - Autres risques liés à la nature, l'étendue, les circonstances et la finalité du traitement, notamment car:
    - traitement de données sensibles à grande échelle
    - surveillance systématique de grandes parties du domaine public
- Exceptions:
  - obligation légale
  - certification selon l'art. 13 LPD
  - code de conduite selon l'art. 11 LPD

L'analyse d'impact

- Contenu:
  - Description du traitement envisagé
  - Evaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée
  - Mesures prévues pour protéger sa personnalité et ses droits fondamentaux.
- Consultation préalable du PFPDT si risques élevés ressortent de l'analyse d'impact

Annonce des violations de sécurité

- Art. 24 nLPD
- Double annonce:
  - Au PFPDT
    - «Dans les meilleurs délais»
    - Risque élevé vraisemblable pour la personnalité ou les droits fondamentaux
    - Contenu de l'annonce:
      - Nature de la violation
      - Conséquences
      - Mesures prises
  - A la personne concernée
    - Si «nécessaire» à la protection de ses droits ou si le PFPDT l'exige
- Importance d'une enquête interne

Annonce des violations de sécurité

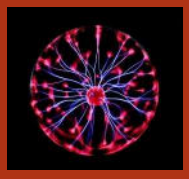
- Exceptions
  - Restrictions du droit d'accès ou obligation de garder le secret
  - Information impossible ou disproportionnée
  - Communication publique suffisante

Les transferts de données à l'étranger

- Le transfert à l'étranger ou à une organisation internationale est possible dans trois cas (art. 6 LPD; art. 16 ss nLPD).
  - L'Etat concerné dispose d'une législation assurant un niveau de protection adéquat
    - Liste du PFPDT
  - A défaut, en présence de garanties appropriées, en particulier:
    - Garanties contractuelles (SCC)
  - Exceptionnellement dans certaines situations particulières
    - Consentement de la personne concernée : très limité, voire exclu en droit du travail
    - Nécessité pour l'exécution du contrat
    - Nécessité à la constatation, à l'exercice ou à la défense de droits en justice
    - Nécessité pour des motifs importants d'intérêt public

Droit à la portabilité

- Art. 28 et 29 nLPD
  - Format électronique couramment utilisé
  - Uniquement pour les données traitées de façon automatisées
- Transfert possible à un autre responsable du traitement
- Droit gratuit
- Restrictions possibles aux mêmes conditions que pour le droit d'accès



Exemples d'application

- Proportionnalité
  - Durées de conservation
  - Casier judiciaire
  - Attestation d'absence de poursuites
  - Questions aux candidat.e.s
  - Tests psychologiques
  - Surveillance
  - Enquêtes internes
- Information
  - Règlement d'entreprise
  - Information *ad hoc*
- Finalité
  - Enquêtes internes
  - Surveillance
  - Utilisation pour les «employés-consommateurs»

QUE TIRER D'AUJOURD'HUI?

41

- Merci pour votre attention!
- Des questions?

David Raedler

Av. Sévelin 15
CP 851
1001 Lausanne

T 021 310 73 10
F 021 310 73 11

www.hdclegal.ch
raedler@hdclegal.ch

@DaRaedler

42