

Journée du CERT 2024

Principes généraux et nouveautés de la LPD révisée

Sylvain Métille

Professeur associé, docteur en droit, avocat au barreau
Université de Neuchâtel, le 26 avril 2024


Au programme

1. Principes généraux
 - Licéité
 - Bonne foi
 - Proportionnalité
 - Transparence
 - Exactitude
 - Finalité
 - Sécurité
2. Nouveautés de la LPD (pour les privés)
 - Notion de données personnelles (art. 2 LPD)
 - Registre des activités de traitement (art. 12 LPD)
 - Analyse d'impact relative à la protection des données (art. 22s LPD)
 - Devoir d'informer (art. 19 ss LPD)
 - Décisions individuelles automatisées (21 LPD)
 - Annonce des violations de la sécurité des données (art. 24 LPD)
 - Représentant (art. 14 LPD)
 - Protection des données dès la conception et par défaut (art. 7 LPD)
 - Droit à la portabilité des données (art. 28 LPD)
 - Dénonciation et enquête du PFPDT (art. 49 ss LPD)
 - Contraventions pénales (60 ss LPD)
 - Et dans une moindre mesure aussi contrat de sous-traitance (art. 9 LPD), communication de données personnelles à l'étranger (art. 16s LPD), droit d'accès (art. 25 LPD), etc.



1. Les principes

Les principes : pas de changement

- Art. 6 et 8 LPD : licéité, bonne foi, proportionnalité, transparence, exactitude, finalité et sécurité.
-  Protection des données dès la conception et protection des données par défaut (art. 9 LPD) ne sont pas des principes, mais des obligations.

Les principes : pas de changement

- La violation des principes constitue une atteinte à la personnalité (art. 30 al. 2 LPD, présomption irréfragable).
- L'atteinte peut être justifiée (licite) par un motif justificatif (art. 31 LPD).
- Il n'y a pas besoin de justification systématique des traitements (≠RGPD) ni besoin de consentement systématique en cas de traitement de données sensibles.



2. Les (principales) nouveautés

Champ d'application (art. 2s LPD)

- La LPD s'applique aux traitements de données personnelles concernant des personnes physiques.
 - Les personnes morales demeurent protégées par les art. 28 ss CC et 13 Cst.



Registre des activités de traitement (art. 12 LPD)

- La déclaration des fichiers au PFPDT a été supprimée, mais le responsable du traitement et le sous-traitant doivent tenir un registre des activités de traitement.
 - Sauf pour les personnes physiques et les entreprises de moins de 250 personnes (et pour autant que le traitement ne porte pas sur des données sensibles à grande échelle ou constitue un profilage à risque élevé)

Analyse d'impact (art. 22s LPD)

- En cas de risque élevé, notamment
 - recours à de nouvelles technologies,
 - traitement de données sensibles à grande échelle,
 - surveillance systématique de grandes parties du domaine public.
- Le responsable du traitement doit réaliser une analyse d'impact avant le traitement et décrire le traitement, les risques pour la personnalité et les droits fondamentaux, ainsi que les mesures prévues.
- Le PFPDT doit être consulté en cas de risques résiduels (*sauf si le conseiller a été consulté*).

Devoir d'informer (art. 19s LPD)

- Le responsable du traitement doit informer la personne concernée lors de toute collecte de données personnelles :
 - son identité et ses coordonnées, la finalité du traitement, les (catégories de) destinataires, les (catégories de) données, les États dans lesquels les données sont traitées (et les garanties).
- Information dans un délai d'un mois si les données ne sont pas collectées directement auprès de la personne concernée.
- Exceptions si le traitement est prévu par une loi, si la personne est déjà informée, si l'information est impossible à donner, etc.
- Ne pas confondre information et consentement au traitement : pas besoin d'accepter l'information.



Annonce des violations de la sécurité des données (art. 24 LPD)

- En cas de violation de la sécurité des données (surtout confidentialité et intégrité), le responsable du traitement doit informer dans les meilleurs délais :
 - le PFPDT s'il existe un risque élevé,
 - les personnes concernées si leur protection l'exige.
- Le sous-traitant doit informer le responsable du traitement indépendamment du risque.



- Pas d'information du PFPDT si le risque n'est pas élevé ou pas vraisemblable.

Décisions individuelles automatisées (art. 21 LPD)

- Décision prise exclusivement sur la base d'un traitement de données personnelles automatisé (informatique) et qui a des effets juridiques pour la personne concernée ou l'affecte de manière significative.
- Devoir d'informer*
- Droits de
 - faire valoir son point de vue*,
 - exiger que la décision soit revue par une personne physique*,
 - connaître la logique sur laquelle se base la décision (droit d'accès).
- *Sauf si la personne concernée a expressément consenti à la prise d'une décision automatisée ou que cette décision est en lien avec un contrat et que la personne concernée est entièrement satisfaite.





Représentant (art. 14 LPD)

- Le responsable du traitement privé qui a son siège ou son domicile à l'étranger doit désigner un représentant en Suisse si :
 - il traite régulièrement et à grande échelle des données personnelles concernant des personnes en Suisse,
 - le traitement présente un risque élevé pour la personnalité des personnes concernées ; et
 - le traitement est en rapport avec l'offre de biens ou de services ou le suivi du comportement de personnes en Suisse.

Droit à portabilité (art. 28 LPD)

- Droit à la remise ou à la transmission à un autre responsable du traitement
- Dans un format électronique courant
- Des données «communiquées»
 - données mises délibérément à la disposition du responsable du traitement et en connaissance de cause par la personne concernée
 - données collectées par le responsable du traitement en lien avec son comportement dans le cadre de l'utilisation d'un service ou d'un appareil
- Conditions
 - traitement automatisé
 - données traitées avec le consentement de la personne* ou en lien avec un contrat.



* Condition insolite (pourquoi faudrait-il une atteinte à la personnalité pour avoir droit à la remise de ses données ?)

Enquête et mesures administratives (art. 49 ss LPD)



- Le PFPDT ouvre d'office ou sur dénonciation une enquête si des indices suffisants font penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données. Il peut renoncer à lorsque la violation est de peu d'importance.
 - Il n'y a pas d'exigence d'erreur système ou de grand nombre de personnes touchées.
- Le PFPDT peut ordonner des mesures administratives (modification, suspension ou cessation de tout ou partie du traitement, effacement ou destruction de tout ou partie des données personnelles) sujettes à recours, mais pas d'amende administrative.

Procédure civile



- Il n'y a pas de frais judiciaires (ni de sûretés en garantie des dépens) dans la procédure relative à un litige relevant de la LPD (procédure de conciliation et procédure au fond).
- Les dépens (et les frais d'avocats) demeurent.



Contraventions pénales (art. 60 ss LPD)



26 avril 2024

S. Métille - Principes et nouveautés

17



- Amende jusqu'à CHF 250'000.- en cas de violation intentionnelle des obligations d'informer, de renseigner et de collaborer, ainsi que des devoirs de diligence (communication à l'étranger, sous-traitance et exigence minimales de sécurité)
 - personnes physiques, exceptionnellement des personnes morales (max. CHF 50'000.- et mesures d'enquête disproportionnées).
- Violation du devoir de discrétion (révélation intentionnelle de données personnelles secrètes connues dans l'exercice d'une profession qui en requiert la connaissance).
 - pas limité aux données sensibles
 - communication au sein d'une entreprise peut réaliser l'infraction

Conclusion (1) : constats

- La LPD a évolué mais sa systématique et ses principes n'ont pas changé.
- Il y a de nouvelles obligations et de nouveaux droits (information étendue, registre, annonce des violations, représentant, AIPD, décision automatisée, portabilité).
- Le PFPDT est un peu plus fort (décisions contraignantes), mais pas trop (pas d'amendes administratives). L'accès à la procédure civile est (un peu) facilité et les sanctions pénales sont (un peu) dissuasives.

26 avril 2024

S. Métille - Principes et nouveautés

18



Conclusion (2) : recommandations

- Toujours penser au respect des principes (respect de la personnalité et conformité matérielle) !
- Vérifier le respect de la LPD dans son ensemble, et ne pas se contenter des nouveautés de septembre 2020 ou des différences avec le RGPD.
- Ce n'est pas qu'une question de droit (tout ce qui est légal n'est pas bon à prendre) mais aussi de respect des personnes.



26 avril 2024

S. Métille - Principes et nouveautés

19

