Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

La révision de la loi fédérale sur la protection des données

Les rendez-vous de la protection des données,
Genève, 15 mars 2018

Jean-Philippe Walter, Dr. en droit

Préposé fédéral suppléant à la protection des données et à la transparence

I. Introduction
II. But, Champ d'application, définitions
III. Principes de base et licéité du traitement
IV. Transparence et droits des personnes concernées
V. Autoréglementation
VI. Obligation du responsable de traitement
VII. Flux transfrontières de données
VIII. Préposé fédéral à la protection des données et à la transparence
IX. Appréciations

I. Introduction

Agenda

- Publication du projet par le CF le 15 septembre 2017
- A partir novembre 2017, examen par le Parlement
- Entrée en vigueur prévue en ?.

Pourquoi réviser ?

- LPD du 16 juin 1992 : loi de première génération
- Nécessité d'adapter au développement technologiques: Émergence de l'internet, des objets connectés, intelligence artificielle, mégadonnées, …
- Mondialisation
- Révision du cadre juridique de l'UE
- Modernisation de la Convention 108

Objectifs

- Adaptation aux technologies et société actuelle
- Renforcer la protection des données
- Renforcer la compétitivité de la Suisse, notamment renforcer de l'attractivité de notre pays pour le numérique
- Permettre de ratifier la Convention 108 modernisé
- Transposer la directive UE 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale et d'entraide en matière pénale
- Permettre un rapprochement de notre niveau de protection des données à celui du règlement UE 2016/670 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel
- Maintenir la reconnaissance d'un niveau de protection adéquat

Renforcer la protection des données

- Améliorer la transparence des traitements
- Améliorer le contrôle que les personnes peuvent exercer sur leurs données
- Préciser et étendre les obligations des responsables de traitement
- Renforcer les compétences et pouvoirs du Préposé fédéral
- Revoir et étendre les sanctions pénales

Lignes générales

- Approche fondée sur le risque
  - Obligations plus strictes pour les traitements à risque élevé

- Approche technologiquement neutre
  - Ne pas bloquer l'innovation
  - S'adapter à l'évolution

- Encouragement à l'autorégulation

II. But, champ d’application, définitions

But

- Protéger la personnalité et les droits fondamentaux des personnes dont les données font l'objet d'un traitement

«Derrière chaque donnée personnelle, il y a un être humain !»

Champ d'application

- Traitement de données concernant des personnes physiques
  - Par des personnes privées
  - Par des organes fédéraux
- Ne s'applique pas au traitement
  - Concernant des **personnes morales**
  - Effectué par une personne physique pour un usage exclusivement personnel
  - Effectué par les Chambres fédérales
  - Effectué par organisations internationales
  - Effectué dans le cadre de procédures juridictionnelles

Définitions

- Élargissement du catalogue des données sensibles: **données génétiques + données biométriques**
- Remplacement de la notion de profil de la personnalité par celle de **profilage**
- Définition de la **violation de la sécurité des données**
- Remplace la notion de maître de fichier par celle de responsable de traitement (RT)
- Introduction de la définition de sous-traitant (ST)
- Abrogation de la définition de fichier

III. Principes de base et Licéité du traitement

- Principe du traitement
- Licéité du traitement par des personnes privées
- Licéité du traitement par des organes fédéraux
- Communication de données par des organes fédéraux

Principes du traitement

- Licéité
- Bonne foi
- Proportionnalité
- Finalité déterminée et reconnaissable + **ultérieurement compatible**
- **Conservation pour la durée nécessaire au traitement**
- Exactitude
- Sécurité des données

Licéité du traitement par personnes privées

- Traitement ne doit pas porter atteinte illicite à personnalité des personnes concernées:
  - Violation des principes de base
  - Traitement contre volonté expresse personne concernée
  - Communication de données sensibles à des tiers

- Motifs justificatifs
  - Consentement
  - Intérêt public ou privé prépondérant
  - Loi

Licéité du traitement par organes fédéraux

- Existence d'une base légale
  - Loi au sens formel si:
    - Données sensibles
    - Profilage
    - Risque d'atteinte grave aux droits fondamentaux de la personne concernée
  - Exceptions :
    - Indispensable à l'accomplissement d'une tâche définie dans loi au sens formel et
    - Pas de risques particuliers pour les droits fondamentaux des personnes concernées
- Dérogation à exigence base légale
  - Autorisation du CF si absence de menace pour les droits des personnes concernées
  - Consentement ou données rendues accessibles par les personnes concernées
  - Protection de la vie ou de l'intégrité corporelle
  - Autorisation pour essais pilotes

Communication de données par organes fédéraux

- Base légale ou
- Communication dans un cas d'espèce si
  - Indispensable à accomplissement tâches légales du RT ou du destinataire
  - Consentement
  - Protection de la vie ou de l'intégrité corporelle
  - Données rendues accessibles par personnes concernées
  - Refus de consentement pour entraver demandeur de se prévaloir de prétentions juridiques ou de faire valoir autres intérêts légitimes
  - Ltrans: données en rapport avec accomplissement tâches publiques et communication répond à intérêt public prépondérant

Communication

- Sur demande, nom, prénom, adresse et date de naissance d'une personne

- Publication en ligne si base légale pour publication et effacement lorsque intérêt public n'existe plus

- Refus de communication si:
  - Intérêt public important ou intérêt légitime manifeste de la personne concernée l'exige, ou
  - Obligation légale de garder le secret ou une disposition particulière de protection des données l'exige

IV. Transparence et droits des personnes concernées

- Devoir d'informer lors de la collecte
- Devoir d'informer en cas de décision automatisée
- Droit d'accès
- Autres droits

Devoir d’informer lors de la collecte

- Devoir d’information couvre toute collecte de données
  - Directe ou indirecte
  - Sensibles ou non sensibles

- Objectif:
  - permettre à personne concernée d’exercer ses droits
  - Garantir la transparence du traitement

Étendue minimale de l’information

- Identité et coordonnées du RT
- Finalité du traitement
- Destinataires ou catégories de destinataires
- Lors collecte auprès de tiers, catégories de données traitées
- Lors communication données à l’étranger, nom de l’État ou de l’organisme international en question + garanties prises

Exceptions au devoir d'informer

- Personne concernée dispose déjà des informations
- Traitement est prévu par la loi
- Obligation légale de garder le secret
- Liberté de la presse
- Lors collecte auprès de tiers, information impossible à donner ou nécessite efforts disproportionnés
- Restrictions possibles si:
  - Intérêts prépondérants d'un tiers l'exige
  - Information empêche le traitement d'atteindre son but
  - Secteur privé: intérêt prépondérant du RT et pas communication à tiers
  - Organe fédéral: intérêt public prépondérant du RT ou compromet enquête, instruction ou procédure judiciaire ou administrative

Devoir d’informer en cas de décision automatisée

- Prise de décision exclusivement sur la base d’un traitement automatisé, y c. profilage
- Décision a des effets juridiques sur la personne concernée, ou
- Décision affecte la personne de manière significative

- Exceptions:
  - Relation directe avec conclusion ou exécution d’un contrat
  - Personne a expressément consenti

Droit d'accès

- Droit de demander si des données sont traitées
- Informations sur
  - Identité et coordonnées du RT
  - Données personnelles traitées
  - Finalité du traitement
  - **Durée de conservation ou critères pour fixer cette durée**
  - Origine des données
  - **Existence d'une décision individuelle automatisée et logique sur laquelle se base la décision**
  - Destinataire ou catégorie de destinataires

Restriction au droit d'accès

- Prévue dans loi au sens formel
- Intérêts prépondérants d'un tiers
- Demande manifestement infondée ou procédurière
- Intérêts prépondérants RT privé et pas communication de données à des tiers
- Organes fédéraux:
  - Intérêt public prépondérant (sûreté intérieure ou extérieure)
- Compromission enquête, instruction ou procédure judiciaire ou administrative
- Garantir liberté de la presse

Autres droits

- Droit de demander de **faire valoir son point de vue lors de décision automatisée** et d'exiger que la décision soit revue par une personne physique

- Droit de demander rectification, effacement ou destruction des données

- Droit d'opposition au traitement (opposition à communication dans secteur public)

- Droit d'ester en justice (gratuité de la procédure civile)

- Droit de dénoncer une violation de la loi au Préposé

V. Autoréglementation

- **Code de conduite**: soumission facultative au Préposé: avis Préposé rendu public

- **Certification facultative** des systèmes, produits ou services

- Nomination facultative de **conseiller à la protection des données**:
  - Pas d'obligation de consulter Préposé sur analyse d'impact

VI. Obligation du responsable de traitement

- Obligation de la protection des données dès la conception (**Privacy by design)** et par défaut (**Privacy by default)**
- Obligation de tenir un **registre des activités** de traitement et de le déclarer au Préposé (organes fédéraux)
- Obligation de procéder à une **analyse d'impact** relative à la protection des données personnelles si risque élevé
- **Annonce des violations** de la sécurité des données
- **Information sur demande du Préposé** de certaines communications à l'étranger en l'absence de protection adéquate

Analyse d’impact

- Susceptible d’entraîner un risque élevé pour la personnalité et les droits fondamentaux
  - Risque dépend nature, étendue, circonstances et finalités traitement
    - Traitement de données à grande échelle
    - Profilage
    - Surveillance systématique de grandes parties du domaine public
- Analyse préalable au traitement
  - Description du traitement envisagé
  - Évaluation des risques
  - Mesures prévues pour protéger

Dérogations RT privé

- Traitement en vertu d'une obligation légale
- Certification
- Code de conduite
  - Reposant sur analyse d'impact
  - Prévoyant mesures pour protection
  - Soumis au Préposé

Consultation préalable

- Analyse révèle que traitement présente un risque élevé en l'absence de mesure pour atténuer le risque

- Préposé communique objections dans un délai de deux mois et propose mesures appropriées

- RT privé peut renoncer à consulter s'il a
  - Nommé conseiller à la protection des données et
  - Consulté ce conseiller

VII. Flux transfrontières de données

- Principe du niveau de protection adéquat
  - Décision d'adéquation par le Conseil fédéral
- En l'absence de décision d'adéquation, niveau approprié garanti par
  - Traité international
  - Clauses de protection des données d'un contrat, préalablement communiquées au Préposé
  - Garanties spécifiques élaborées par organe fédéral et préalablement communiquées au Préposé
  - Clauses types de protection des données préalablement approuvées, établies ou reconnues par préposé
  - Règles contraignantes d'entreprises préalablement approuvées par le préposé ou une APD relevant d'un État adéquat

Dérogations

- Personne concernée a expressément consenti à la communication
- Communication en relation directe avec conclusion ou exécution d'un contrat
  - Entre RT et personne concernée
  - Entre RT et cocontractant dans l'intérêt personne concernée
- Communication nécessaire à sauvegarde intérêt public prépondérant
- Communication nécessaire à constatation, exercice ou défense d'un droit devant un tribunal ou une autorité étrangère compétente
- Protection de la vie ou l'intégrité corporelle et consentement ne peut être obtenu
- Données rendues accessibles à tout un chacun et pas opposition au traitement
- Données proviennent d'un registre public prévu par la loi

VIII. Préposé fédéral à la protection des données

Nomination et statut

- Nommé par Conseil fédéral et approbation par Assemblée fédérale
- Mandat de 4 ans renouvelable 2 fois (tacitement)
- Exerce ses fonctions de manière indépendante et sans instructions d'autorité ou de tiers
- Rattachement administratif à la Chancellerie fédérale
- Secrétariat permanent
- Propre budget
- Engage son personnel

Enquête

- D'office ou sur dénonciation si
  - Indices que traitement contraire à dispositions de protection des données
- Peut renoncer à une enquête si violation de peu d'importance
- Obligation de fournir tous les renseignements ou documents nécessaires à l'enquête
- Information de la personne concernée auteur de la dénonciation
  - Suites données à dénonciation
  - Résultats enquête éventuelle

Pouvoirs

- En cas de refus de collaborer, le Préposé peut notamment ordonner:
  - Accès à tous les renseignements, documents, registres des activités et données personnelles nécessaires à l'enquête;
  - Accès aux locaux et installations;
  - Audition de témoins;
  - Expertises
- Peut également ordonner mesures provisionnelles pour la durée de l'enquête et
  - Les faires exécuter par une autorité fédérale ou organes de police cantonaux ou communaux.

Mesures administratives

- En cas violation des dispositions de protection des données, Préposé peut ordonner:
  - Suspension, modification ou cessation du traitement
  - Effacement ou destruction des données personnelles
- Peut suspendre communication à l'étranger si conditions légales pas respectées
- Peut ordonner:
  - Fourniture des informations relatives aux flux transfrontières
  - Prendre les mesures techniques et organisationnelles (sécurité, privacy by design, privacy by default)
  - Informer les personnes concernées (transparence, décision automatisée)
  - Établir analyse d'impact et consultation préposé
  - Informer sur violation de sécurité des données
  - Communiquer les renseignements en application du droit d'accès.

Coordination

- Autorité administrative fédérale exerçant surveillance sur un privé ou organisation extérieure à administration fédérale
  - Préposé se prononce avant décision touchant à questions de protection des données
  - En cas d'enquête contre la même partie, coordination des procédures

Assistance administrative en Suisse

- Autorités fédérales et cantonales communiquent informations et données personnelles nécessaires à l'accomplissement des tâches légales du Préposé

- Le Préposé le fait aux
  - Autorités de protection des données
  - Autorités poursuite pénale compétentes lorsqu'il dénonce infractions
  - Autorités fédérales ou aux polices cantonales et communales dans le cadre exécution mesures provisionnelles qu'il ordonne

Assistance administrative aux autorités étrangères

- Échange d'informations ou données personnelles avec APDs nécessaires à l'accomplissement tâches respectives si:
  - Réciprocité garantie
  - Utilisation uniquement dans le cadre procédure à la base de la demande
  - APD destinataire ne divulgue pas secrets professionnels, d'affaires ou de fabrication
  - Communication à des tiers avec accord préalable de l'autorité qui transmet
  - APD destinataire respecte charges et restrictions d'utilisation exigées par autorité qui transmet
  - Demande d'assistance doit être motivée et contenir des indications nécessaires à son traitement

Autres tâches du Préposé

- Registre des activités de traitement des organes fédéraux
- Rapport d'activité annuel
- Information du public sur ses constatations et décisions
- Information, **formation** et conseil
- Assistance aux organes cantonaux et collaboration avec les APDs suisses et étrangères
- **Sensibilisation** du public, en particulier personnes vulnérables
- Information aux personnes concernées sur l'exercice de leurs droits
- Avis sur les projets législatifs et mesures impliquant le traitement de données
- Tâches en relation avec Ltrans
- **Élaboration des guides et des outils** à l'intention des RT, sous-traitants, personnes concernées

Émoluments

- Prise de position concernant codes de conduite
- Approbation des clauses types et règles contraignantes d'entreprises
- Consultation préalable dans le cadre des analyses d'impact
- Mesures provisionnelles et mesures administratives
- Conseil aux organes fédéraux et personnes privées

Sanctions pénales

- Violation des obligations d'informer, de renseigner et de collaborer
- Violation des devoirs de diligence
- Violation du devoir de discrétion
- Insoumission à une décision du Préposé ou autorité de recours

Amende jusqu'à 250'000 francs

(Possibilité de condamner entreprise si montant de l'amende ne dépasse pas 50'000 Frs)

XI. Appréciations

- Le projet va dans la bonne direction, mais
- Différences terminologiques et matérielles avec la convention 108 modernisée et le RGPD :
  - Insécurité juridique,
  - Complication pour RT soumis au RGPD et LPD
  - Décision d'adéquation
  - Distorsion de concurrence avec UE
  - Meilleure protection pour les citoyens européens dont les données sont traitées en Suisse
- Quelques dispositions non reprises:
  - Droit à la portabilité
  - Droit au déréférencement
  - Obligation de démontrer la conformité : renversement de la preuve
  - Action collective
  - Responsabilité objective du fait du traitement
  - Obligation de soumettre code de bonne pratique au PFPDT
  - Obligation de nommer des conseillers à la protection des données
  - Sanctions administratives dissuasives
  - Certification obligatoire pour traitement à risque particulièrement élevé