Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Le PFPDT et les implications du RGPD en Suisse

Les Rendez-vous de la protection des données du PPDT, 19 mars 2019, Centre de l'Espérance, Genève

Catherine Lennman,
Déléguée aux affaires internationales et à la Francophonie,
Préposé fédéral à la protection des données et à la transparence

Sommaire de l’exposé

I. Protection des données: cadre légal
II. Le PFPDT - présentation générale
III. Incidences du RGPD en Suisse
IV. RGPD: Aspects pratiques choisis
V. Questions ?

I. Protection des données: cadre légal

- Article 8 CEDH

  « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »

- Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) et son Protocole additionnel à la Convention 108 concernant les autorités de contrôle et les flux transfrontières de données.

- Article 13, alinéa 2, Constitution fédérale :

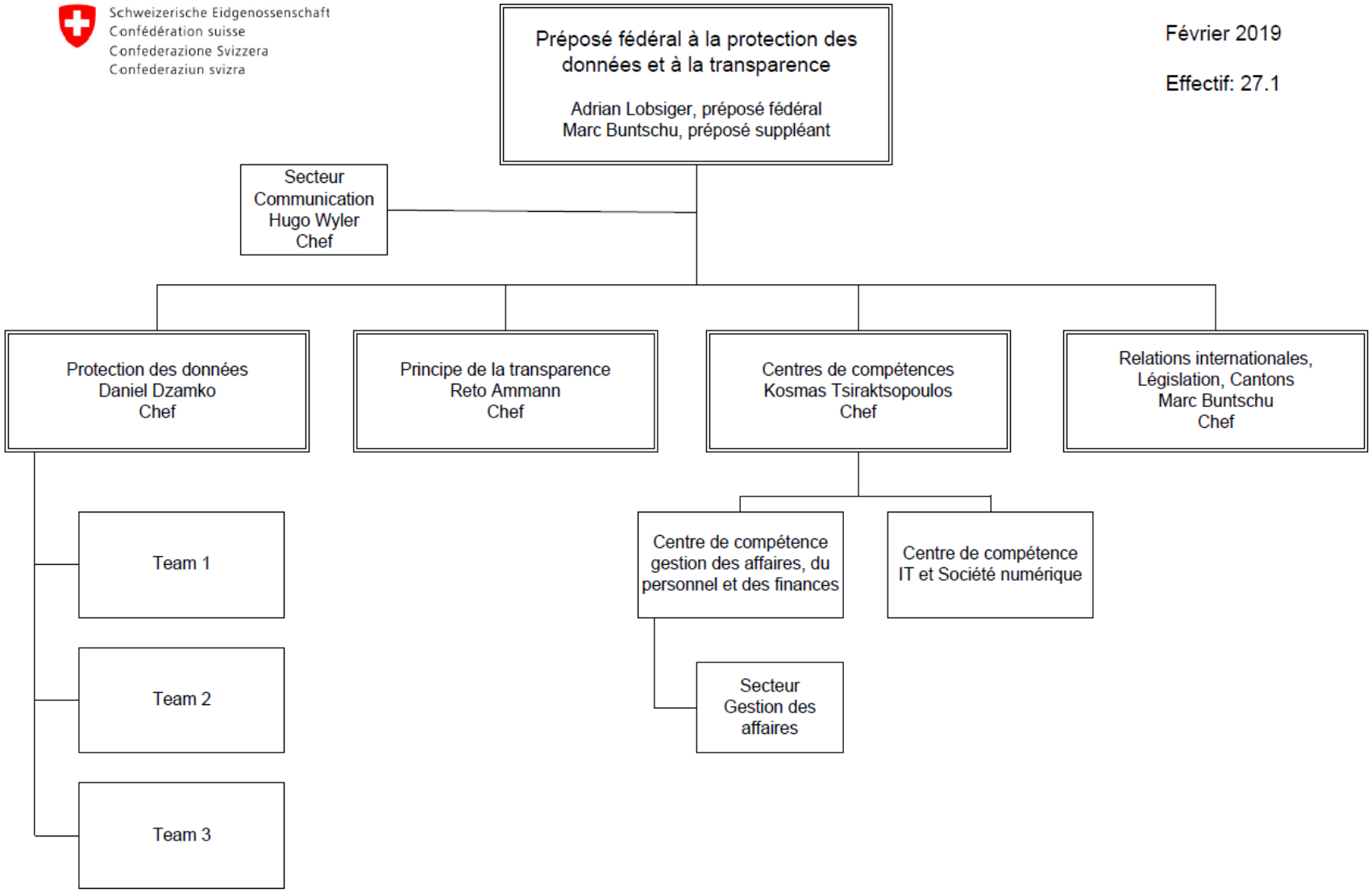
  « Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent »
- Loi fédérale du 19 juin 1992 sur la protection des données
- Lois cantonales de protection des données

- Règlement européen sur la protection des données (Art. 3 § 2)

II. Le Préposé fédéral à la protection des données et à la transparence

Adrian Lobsiger

II. Le secrétariat du PFPDT



II. Les tâches du PFPDT

- Surveillance des **organes fédéraux**
- Surveillance des **personnes privées**
- Conseil aux personnes privées
- Soutien et conseil aux organes fédéraux et cantonaux
- Avis sur les projets législatifs de la Confédération
- **Collaboration** avec les organes de protection des données nationaux et internationaux, ex. autorités cantonales, Convention 108, EDPB, AFAPDP, Conférence Internationale, etc.
- Information / sensibilisation / formation
- Tenue et publication du registre des fichiers

II. Ce que le PFPDT fait

- Émettre des recommandations
- Dénoncer des infractions pénales qui se poursuivent d'office
- Informer le public de ses constatations et de ses recommandations *s'il en va de l'intérêt général* (art. 30 al.2 LPD),
- Qualité pour recourir contre une décision du TAF statuant sur une recommandation (art. 29 al. 4 LPD)

II. Ce que le PFPDT ne fait pas

- Infliger des amendes administratives
  - Ex. CNIL – amende Google
- Sanctionner lui-même pénalement
- **Pas de pouvoir d'approbation préalable**
  - Ex. un système d'autorisation préalable est connu des droits cantonaux, ex. vidéosurveillance
- Agir à la place du citoyen (art. 15, 25 LPD)

Révision de la LPD

- Publication du projet par le CF le 15 septembre **2017**
- 11 janvier 2018: la CIP-N décide de scinder la révision en **deux** étapes.
- 1.3.2019: entrée en vigueur de la LPDS
- Entrée en vigueur de la révision totale?

Pourquoi réviser ?

- LPD du 16 juin 1992: loi de première génération
  - ➢ Nécessité d'adapter aux technologies et société actuelle

- **Renforcer** la protection des données et la compétitivité de la Suisse

- Révision du cadre juridique de l'UE:
  - Transposer la directive UE 2016/680
  - Se rapprocher du règlement UE 2016/679

- Convention 108+

➢ Maintien de la reconnaissance d'un niveau de protection **adéquat.**

III. Implications du RGPD en Suisse

Un cadre unifié

- Réforme globale, qui poursuit **3** objectifs:
  1. **Renforcer** les droits des personnes
  2. **Responsabiliser** les acteurs traitant des données
  3. Établir une **gouvernance nouvelle** de la régulation

- Renforce et consacre les principes :
  - Licéité, loyauté, transparence
  - Limitation des finalités
  - Minimisation des données
  - Exactitude
  - Limitation de la conservation
  - Intégrité et confidentialité
  - Responsabilité

1. Renforcement des droits des personnes

- Consentement renforcé et transparence
- Le droit à la **portabilité** des données
- Le droit à **l'effacement** (« droit à l'oubli »)
- Le droit à la limitation du traitement
- Des conditions particulières pour le traitement des données des **enfants**
- Droit d'opposition et prise de décision individuelle automatisée (y compris le profilage)
- Introduction du principe des **actions collectives**
- Un droit à **réparation des dommages**

2. Responsabilisation des acteurs

- **Transparence et responsabilisation** des acteurs:
  - La protection des données dès la conception et par défaut (*by design and by default*)
  - Un allègement des formalités préalables
  - Des responsabilités partagées et précisées

- Une **boîte à outils** pour la mise en conformité:
  - Le délégué à la protection des données
  - La tenue d'un registre des traitements
  - La notification de failles de sécurité
  - La certification de traitements
  - L'adhésion à des codes de conduites
  - Les études d'impact sur la vie privée

3. Gouvernance nouvelle

- Une **coopération renforcée** entre les autorités :
  - Assistance mutuelle et opérations conjointes
  - « Guichet unique » et autorité « chef de file »
  - Mécanisme de contrôle de la cohérence
  - Le Comité européen à la protection des données (CEPD)
- Des **sanctions** encadrées, graduées et renforcées

Une application territoriale élargie (I)

- L'ancienne directive 95/46/CE s'appliquait au traitement effectué dans le cadres des activités d'un établissement du RT **sur le territoire d'un État membre** (art. 4 § 1 lit. a).

- En 2014, dans le cas «Google Spain» (C-131/12), la CJUE s'est prononcée pour l'application territoriale de la directive aux traitements réalisés par **Google Inc. (USA)**.

- Lors de l'élaboration du RGPD, le législateur a repris cette décision afin de mieux protéger les données des européens et prévoyant une **application extraterritoriale** du nouveau règlement.

Une application territoriale élargie (II)

1. Critère du rattachement = lieu d'établissement du responsable du traitement ou d'un sous-traitant

- Traitements effectués dans le cadre des activités d'acteurs établis sur le territoire de l'UE…
- …qu'ils aient ou non lieu dans l'UE

➢ Critère décisif = existence d'un établissement dans l'UE.

- ✓ Dispositif stable
- ✓ Exercice effectif et réel d'une activité
- ✓ Traitement effectué dans le cadre des activités

📖 Cas *Weltimmo c. NAIH* (C-230/14)

Une application territoriale élargie (III)

2. Critère du ciblage = lieu de situation des personnes concernées par le traitement

- Traitements effectués par des acteurs non établis sur le territoire de l'UE dès lors **qu'ils visent** des personnes se trouvant sur le territoire de l'UE
  - Offre de biens et services
  - Suivi de comportements au sein de l'UE

➢ Seul compte le **lieu de situation de la personne concernée** par le traitement (≠ nationalité UE).

📖 Cas *Hotel Alpenhof c. Heller (C-585/08)*

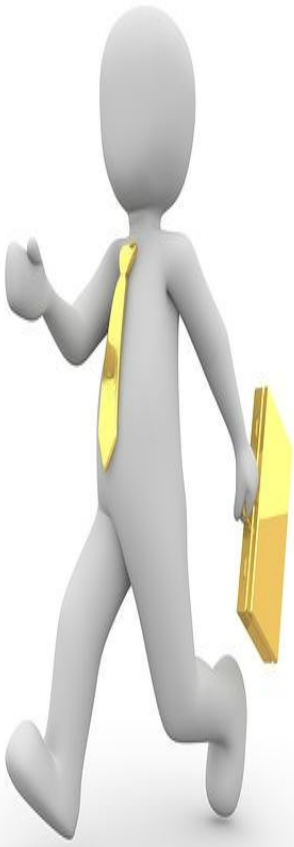
Article 3 RGPD et cons. 23

- Visent à clarifier la situation;
- Approche pragmatique;
- Consultation publique jusqu'au 18 janvier 2019.
- Version finale: été 2019.

Le Représentant – Art. 27 RGPD

Lorsque le responsable de traitement ou le sous-traitant qui n'est **pas établi dans l'UE** entre **dans le champ d'application** du RGPD

- Personne physique ou morale ✓
- Désigné par un mandat **écrit** ✓
- Pour le compte de plusieurs RT/ST ✓
- Personnes concernées doivent être informées ✓



- Tient un registre des traitements ✓
- Coopère avec les APD ✓
- Incompatible avec le rôle de délégué à la pdd ✓
- Exceptions art. 27 § 2 RGPD ✓

Mesures coercitives possibles contre le représentant!

Sanctions encadrées, graduées et renforcées

- **Actions correctrices** (art. 58 RGPD), p. ex:
  - Prononcer un avertissement;
  - Limiter temporairement ou définitivement un traitement;
  - Ordonner la rectification, la limitation ou l'effacement.

- **Amendes administratives** (art. 83 RGPD)
  - Jusqu'à **20 millions** d'euros ou, dans le cas d'une entreprise, jusqu' à **4% du chiffre annuel mondial.**
  - Critère d'appréciation pour le prononcé d'amendes
  - Niveaux de sanction renforcés et gradués.

IV. Aspects pratiques choisis: rappel des exigences principales du RGPD

1. **Registre de conformité** (art. 30)
2. Respect des principes généraux (art. 5ss)
3. Informations des personnes concernées (art. 13ss)
4. Respect des droits des personnes concernées (art. 12ss)
5. Sous-traitants (art. 28)
6. Sécurité des données et Analyse d'impact (art. 24, 32ss)
7. Notification d'une violation (art. 33)
8. Organisation (représentant [art. 27ss], délégué à la protection des données [art. 37ss])

Registre des activités de traitement (I)

- **Outil de pilotage** de la protection des données destiné à:
  1. Mieux connaître, gérer et piloter la stratégie de p.d.d.
  2. Faciliter la gestion des demandes des utilisateurs
  3. Préciser les mesures de sécurité adoptées en cas de faille /piratage.

- Obligatoire tant pour le RT que le ST.

- Exception pour les sociétés < 250 employés, sauf si le traitement:
  - Comporte un risque pour les droits et libertés
  - S'il n'est pas occasionnel
  - S'il porte sur des catégories particulières ou pénales.

IV. RGPD en pratique : conséquences pour les sites web (I)

- **Minimisez les données personnelles que vous collectez!**

- **Informez** vos clients sur ce que vous faites de leurs données! Soyez concis et compréhensible .

- et assurez la **transparence** !

IV. RGPD en pratique : conséquences pour les sites web (II)

1. **Demander le consentement (éclairé)**
   - De manière **explicite (acte positif clair)**
   - Doit pouvoir être **retiré à tout moment**.
   - Les **mineurs** font l'objet d'un traitement spécifique
   - Pour la collecte/traitement des **données personnelles** telles que: nom, prénom, adresse IP, tél, cookies, etc.
   - **Pour l'ensemble des services du site web:** Google analytics, Adsense, Adwords, Facebook, Twitter..

2. **Modalité de la demande**
   - **Dissociée:** distinctes des autres termes et conditions
   - **Active:** pas de cases pré-cochées
   - **Granulaire:** par type de traitement
   - **Facile à retirer:** informer et disposer de mécanismes

IV. RGPD en pratique : conséquences pour les sites web (III)

3. **Preuve**
   - RT : preuve consentement
   - Pas de forme définie
4. **Durée du consentement**
   - Pas de limite de validité
   - Tant que l'utilisateur ne change pas d'avis
   - Nouveau service = nouvelle demande de consentement
5. **Formulaire**
   - Indiquez durée de conservation et finalités.
   - Mentionnez si vous conservez l'adresse IP.
   - Liens vers **mention légale** possible.

IV. RGPD en pratique : conséquences pour les sites web (IV)

6. Attention aux cookies ou traceurs publicitaires!

- Si possible, privilégier la publicité sémantique!
- Selon l'objet du traceur, il conviendra soit:
  - d'informer (ex. cookie panier d'achat) ou
  - d'obtenir le consentement (ex. cookie lié à une opération publicitaire) avant le dépôt/lecture.

➢ **7 mars 2019**

AUTORITEIT PERSOONSGEGEVENS

V. Questions

Merci !

?

- catherine.lennman@edoeb.admin.ch

www.edoeb.admin.ch

www.thinkdata.ch