Que doit donc contenir le règlement de traitement d'un organe fédéral?

Le règlement de traitement vise en premier lieu à rendre le développement de systèmes et le traitement de données aussi transparents que possible. La première version du règlement est disponible à la fin des phases de planification du projet (phase de conception resp. évaluation selon HERMES[1]). Ce règlement est ensuite continuellement mis à jour durant l'exploitation du système. Les modifications apportées au système et les contrôles opérés sur ce dernier doivent en particulier être dûment documentés. Le règlement de traitement doit être établi sous une forme aussi compacte et compréhensible que possible (autant que nécessaire, mais le moins possible), de manière à ce que le système puisse être compris et jugé par des personnes «non expertes» dans le domaine. Pour les informations de détail, on peut en principe se contenter de références aux documents existants.

Le règlement de traitement (art. 21 et 16 de l'ordonnance relative à la loi fédérale sur la protection des données, OLPD, RS 235.11) comporte au moins les points suivants:

- **Table des matières**
- **Abréviations utilisées**
- **Modifications du règlement**

1. **les nom et adresse de l'organe fédéral responsable (art. 16, al. 1, let. a, OLPD)**

2. **le nom et la dénomination complète du fichier (art. 16, al. 1, let. b, OLPD)**

3. **la base juridique et le but du fichier (art. 16, al. 1, let. d, OLPD)**

4. **la situation de départ**
   Décrire brièvement pourquoi le système doit être développé, de même que le but précis du projet et l'état final à atteindre.

5. **les catégories de données personnelles traitées (art. 16, al. 1, let. e, OLPD)**

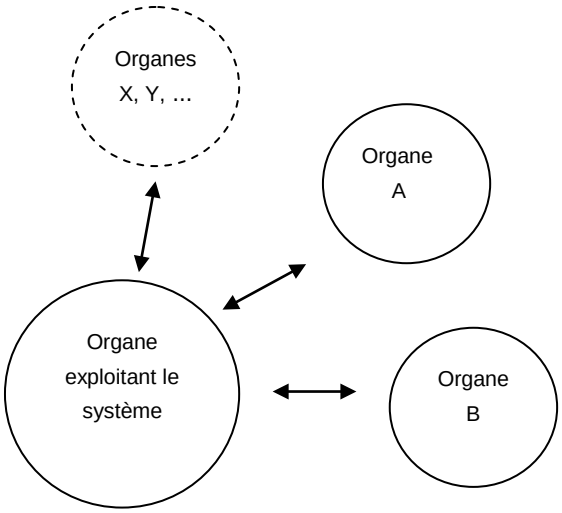
6. **les catégories des destinataires des données (art. 16, al. 1, let. f, OLPD)**

7. **les catégories de participants au fichier, c'est-à-dire les tiers qui sont en droit d'introduire des données dans le fichier ou d'y procéder à des mutations (art. 16, al. 1, let. g, OLPD)**

8. **la documentation des unités d'organisation concernées par le système**
   (Organe exploitant le système[2] – Environnement)

[1] HERMES est un standard de l'Administration fédérale suisse pour la conduite et le développement de projets. D'autres méthodes de conduite de projets peuvent être utilisées dans l'économie privée.
[2] «Système» ne doit pas être ici compris sous l'acception technique de l'informatique.

Feldeggweg 1, 3003 Berne
Tél. 058 462 43 95, Fax 058 465 99 96
www.edoeb.admin.ch



Description des interfaces:

De	À	**But**	**Type données**	**Périodicité**	**Initiateur (unité admin.)**	**Media**
Exploitant	Organe A		Texte, sensible	Mensuel		Papier
Organe A	Exploitant		...	...	...	...
Organe X	Exploitant	...	...	...	...	Courriel

...

Pour chaque communication (transfert) de données, les informations suivantes doivent être précisées:

- D'où proviennent les données?
- Qui reçoit les données?
- Dans quel but les données sont-elles communiquées?
- Quelles données sont communiquées ?
- À quelle fréquence les données sont-elles communiquées?
- Qui initie la communication?
- Au moyen de quel support (média) les données sont-elles communiquées?

Le «graphique à bulles» ci-dessus délimite la table de description des interfaces.

8.1 Organigramme de l'organe exploitant le système

Représentation de l'organigramme et des unités (y compris le nombre de collaborateurs) qui travaillent avec le système.

8.2 Responsabilités

Consigner, qui est responsable de l'application, du réseau, de la base de données et du système d'exploitation, etc.

8.3 Autres applications importantes de l'exploitant ayant des interfaces avec le système présenté dans le présent règlement

Lister ces applications avec leur interconnexion avec le système en question.

9. Dossier de la documentation de planification, réalisation et exploitation du fichier

Planification: étude préalable, conception, ...

Réalisation: Documentation de l'application (basée sur un cahier des charges)

Exploitation: Manuels d'utilisation et d'administration, ...

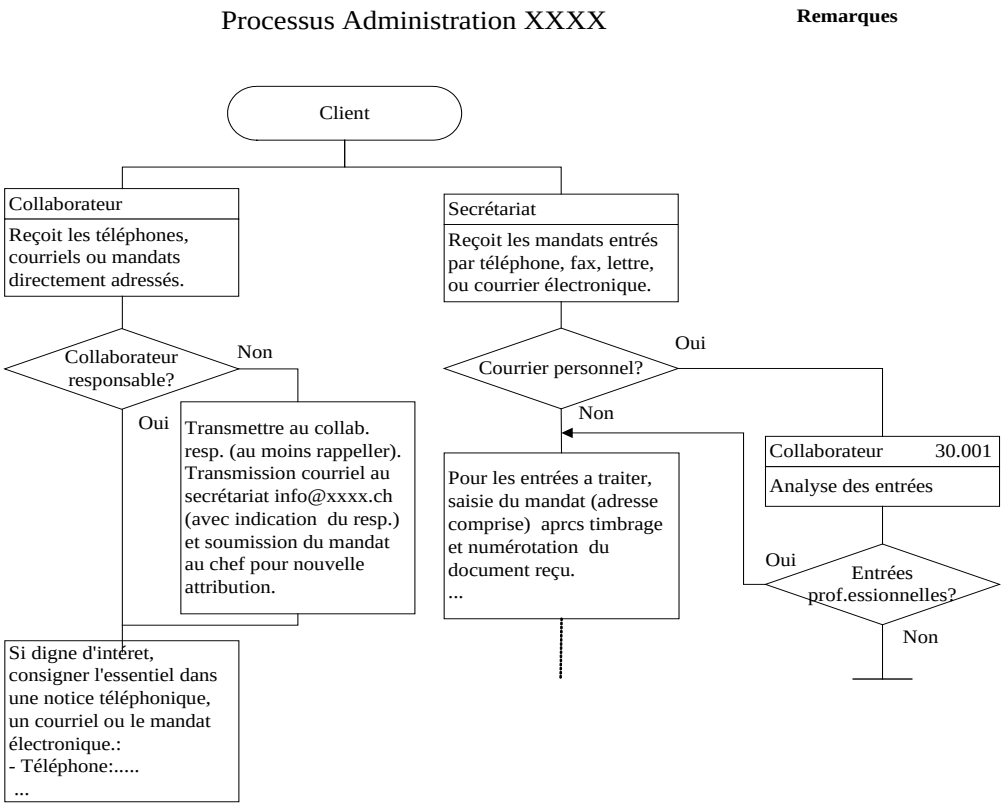
10. Déclaration du fichier au PFPDT (art. 16 OLPD)

Les organes fédéraux (cf. art. 11a de la loi sur la protection des données, LPD, RS 235.1) doivent annexer la copie de la déclaration ordinaire au règlement. L'annonce ou la mise à jour doit être effectuée dans les trois langues nationales pour l'administration fédérale. Les organes fédéraux déclarent généralement leurs fichiers via l'intranet. D'autres informations concernant la déclaration sont fournies sur le site internet du PFPDT: www.leprepose.ch > Protection des données > Déclaration des fichiers.

11. Processus

Les processus doivent être documentés avec un niveau de détails proportionnel à la sensibilité des données traitées (aussi précis que nécessaire pour assurer la transparence requise).

Exemple de documentation d'un processus:



12. **Organe responsable de la protection et de la sécurité des données** (art. 21, al. 2, let. a, OLPD)

13. **La provenance des données** (art. 21, al. 2, let. b, OLPD)

    … devrait être évidente à partir de la description des interfaces.

14. **Les buts dans lesquels les données sont régulièrement communiquées** (art. 21, al. 2, let. c, OLPD)

    … devraient être évidents à partir de la description des interfaces.

15. **Procédures de contrôle et en particulier mesures techniques et organisationnelles visées à l'art. 20 OLPD** (art. 21, al. 2, let. d, et 8 à 10 OLPD)

    Il s'agit de décrire les procédures de contrôle introduites durant les phases de planification, réalisation et exploitation du projet.

    Mesures techniques et organisationnelles

    Selon le point de vue considéré, les huit objectifs ci-dessous peuvent en partie se recouper. Pour chacun d'eux, il faut déterminer les mesures adéquates à prendre. Le point 19 (configuration des moyens informatiques) peut également contenir des informations à ce sujet.

    Contrôle des installations à l'entrée: (art. 9, al. 1, let. a, OLPD)

    les personnes non autorisées n'ont pas accès aux locaux et aux installations utilisées pour le traitement de données personnelles;

    Contrôle des supports de données personnelles: (art. 9, al. 1, let. b, OLPD)

    les personnes non autorisées ne peuvent pas lire, copier, modifier ou éloigner des supports de données;

    Contrôle du transport: (art. 9, al. 1, let. c, OLPD)

    les personnes non autorisées ne peuvent pas lire, copier, modifier ou effacer des données personnelles lors de leur communication ou lors du transport de supports de données*;*

    Contrôle de communication: (art. 9, al. 1, let. d, OLPD)

    les destinataires auxquels des données personnelles sont communiquées à l'aide d'installations de transmission peuvent être identifiés*;*

    Contrôle de mémoire: (art. 9, al. 1, let. e, OLPD)

    les personnes non autorisées ne peuvent ni introduire de données personnelles dans la mémoire ni prendre connaissance des données mémorisées, les modifier ou les effacer;

    Contrôle d'utilisation: (art. 9, al. 1, let. f, OLPD)

    les personnes non autorisées ne peuvent pas utiliser les systèmes de traitement automatisé de données personnelles au moyen d'installations de transmission;

    Contrôle d'accès: (art. 9, al. 1, let. g, OLPD)

    les personnes autorisées ont accès uniquement aux données personnelles dont elles ont besoin pour accomplir leurs tâches;

    Contrôle de l'introduction (journalisation): (art. 9, al. 1, let. h, OLPD)

    l'identité des personnes introduisant des données personnelles dans le système, ainsi que les données introduites et le moment de leur introduction peuvent être vérifiés a posteriori (des procès-verbaux de journalisation ne doivent être établis qu'en cas de nécessité, après en avoir dûment informé les personnes concernées).

16. **Description des champs de données et des unités d'organisation qui y ont accès** (art. 21, al. 2, let. e, OLPD)

    Une matrice de droits doit définir quels rôles (utilisateurs) possèdent quels accès (lire, muter, détruire,…) à quelles données.

17. **Nature et étendue de l'accès des utilisateurs au fichier** (art. 21, al. 2, let. f, OLPD)

    Il s'agit de décrire, par qui et comment les données peuvent être consultées (sélectionnées) et si l'accès à ces dernières est partiel ou complet.

18. **Procédures de traitement des données, notamment les procédures de rectification, blocage, anonymisation (pseudonymisation), sauvegarde, conservation, archivage ou destruction des données** (art. 21, al. 2, let. g, OLPD)

    La plupart des exigences ci-dessus devraient être déjà couvertes dans la documentation des processus (cf. point 11). Seuls les processus qui n'auraient pas encore été décrits doivent être documentés ici.

    Il faut mettre en place les outils et les procédures permettant l'exercice du droit de faire rectifier ou détruire des données personnelles, d'en faire interdire la communication ou d'en faire mentionner le caractère litigieux (art. 25 et 20 LDP). Tout refus ou restriction des droits opposé à la personne concernée doit lui être notifié par voie de décision.

    Le traitement commence par la collecte des données personnelles et se termine par leur archivage ou destruction.

19. **Configuration des moyens informatiques** (art. 21, al. 2, let. h, OLPD)

    - Application
    - Réseau
    - Base de données
    - Système d'exploitation
    - Hardware

    L'idée est ici de décrire les mesures de protection et sécurisation des données à caractère informatique qui peuvent être prises dans un des cinq niveaux systémiques ci-dessus.

20. **Procédure d'exercice du droit d'accès** (art. 21, al. 2, let. i, 8 et 9 LPD, et 13 OLPD)

    Il s'agit en particulier d'indiquer à qui doit s'adresser la personne faisant valoir son droit d'accès et comment se déroule précisément ce processus (y compris la phase de la décision).

Annexe 1 *Copie de la déclaration ordinaire du fichier*

Annexe 2 *Les trois principaux masques de saisie de l'application*

Etat: mai 2014