

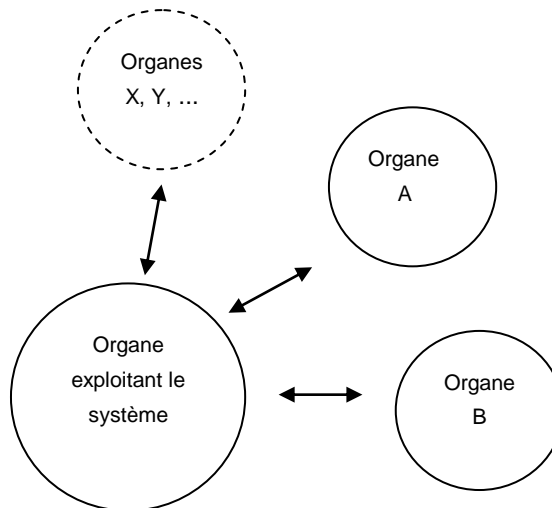


Que doit donc contenir un règlement de traitement?

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 HERMES¹). 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. 11 et 21 OLPD) comporte les points suivants:

	Page
Abréviations utilisées	x
Modifications du règlement	x
1. Point de départ	x
Décrire brièvement pourquoi le système doit être développé, de même que le but précis du projet et l'état final à atteindre.	
2. Documentation des unités d'organisation concernées par le système (Organe exploitant le système ² – Environnement)	x



¹ Standard ouvert de l'Administration fédérale pour la conduite et le développement de projets en technologie de l'information et de la communication. 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.



Description des interfaces:

De	À	But	Type données	Périodicité	Initiateur	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?

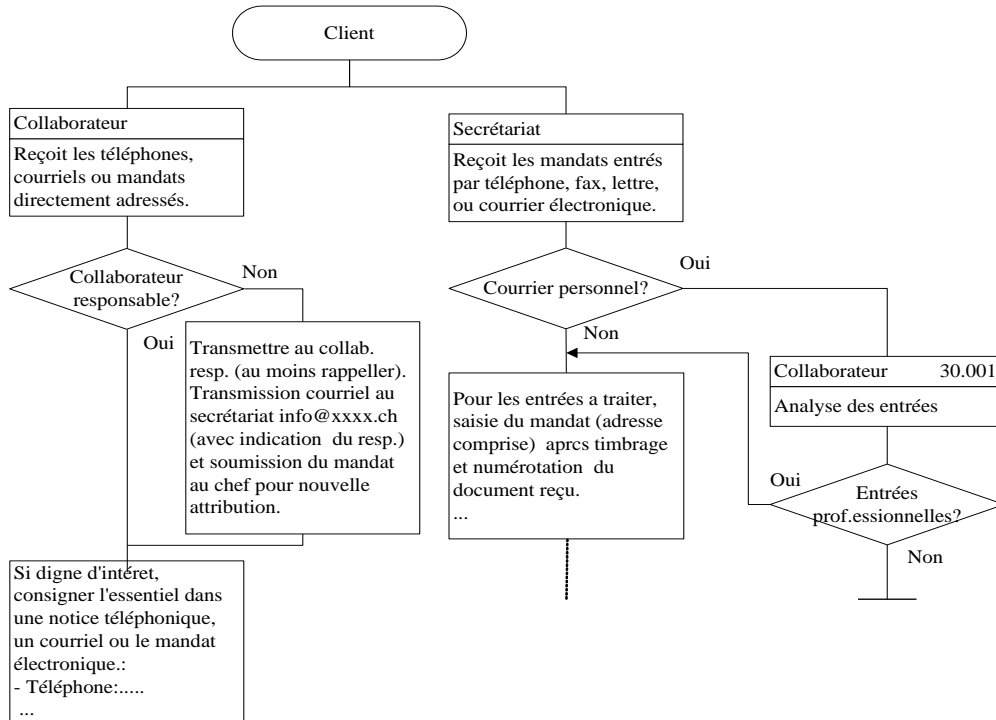
Le «graphique à bulles» ci-dessus délimite la table de description des interfaces.

- 2.1 Organigramme de l'organe exploitant le système X**
Représentation de l'organigramme et des unités (y compris le nombre de collaborateurs) qui travaillent avec le système.
- 2.2 ResponsabilitésX**
Consigner, qui est responsable de l'application, du réseau, de la base de données et du système d'exploitation, etc.
- 2.3 Autres applications importantes de l'exploitant ayant des interfaces avec le système présenté dans le présent règlementX**
Lister ces applications avec leur interconnexion avec le système en question...
- 3. Dossier de la documentation de planification, réalisation et exploitation du fichierX**
Planification: étude préalable, conception, ...
Réalisation: Documentation de l'application (basée sur un cahier des charges)
Exploitation: Manuels d'utilisation et d'administration, ...
- 4. Déclaration du fichier au PFPD (Art. 16 OLPD)X**
Annexer la copie de la déclaration ordinaire au présent règlement.
L'annonce ou la mise à jour doit être effectuée dans les trois langues nationales pour l'administration fédérale et les grandes entreprises. Elle s'effectue sur le site internet: www.leprepose.ch (rubrique services – protection des données – déclarer un fichier).
- 5. ProcessusX**
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:



Processus Administration XXXX

Remarques



- 6. Organe responsable de la protection et de la sécurité des données**
(Art. 21, Al. 2, Lit. a OLPD) X
- 7. Provenance des données (Art. 21, Al. 2, Lit. b OLPD) X**
... devrait être évidente à partir de la description des interfaces ...
- 8. Buts dans lesquels les données sont régulièrement communiquées**
(Art. 21, Al. 2, Lit. c OLPD)..... X
... devraient être évidents à partir de la description des interfaces ...
- 9. Procédures de contrôle et en particulier mesures techniques et organisationnelles visées à l'art. 20 OLPD**
(Art. 21, Al. 2, Lit. d et Art. 8 - 10 OLPD) X
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 13 (configuration des moyens informatiques) peut également contenir des informations à ce sujet.

Contrôle des installations à l'entrée: (Art. 9, Al. 1, Lit. 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, Lit. 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, Lit. 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, Lit. 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, Lit. 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, Lit. 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, Lit. 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, Lit. 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).

- 10. Description des champs de données et des unités d'organisation qui y ont accès (Art. 21, Al. 2, Lit. e OLPD)X**
Une matrice de droits doit définir quels rôles (utilisateurs) possèdent quels accès (lire, muter, détruire,...) à quelles données.
- 11. Nature et étendue de l'accès des utilisateurs au fichier (Art. 21, Al. 2, Lit. f OLPD)X**
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.
- 12. Procédures de traitement des données, notamment les procédures de rectification, blocage, anonymisation (pseudonymisation), sauvegarde, conservation, archivage ou destruction des données (Art. 21, Al. 2, Lit. g OLPD) X**
La plupart des exigences ci-dessus devraient être déjà couvertes dans la documentation des processus (cf. point 5). Seuls les processus qui n'auraient pas encore été décrits doivent être documentés ici. Le traitement commence par la collecte des données personnelles et se termine par leur archivage ou destruction.
- 13. Configuration des moyens informatiques (Art. 21, Al. 2, Lit. h OLPD)x**
- 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.

14. Procédure d'exercice du droit d'accès (Art. 21, Al. 2, Lit. i OLPD)x

On souhaite en particulier savoir, à qui doit s'adresser la personne faisant valoir son droit d'accès et comment se déroule précisément ce processus.

Annexe 1 *Copie de la déclaration ordinaire du fichier*

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

Etat: janvier 2012