DIRECTIVES

sur les exigences minimales qu'un système de gestion de la protection des données doit remplir (certification de l'organisation ou de la procédure au sens de l'art. 4 OCPD)

du XX novembre 2007

Le Préposé fédéral à la protection des données et à la transparence,

vu l'art. 11, al. 2, de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[1],

vu l'art. 4, al. 3, de l'ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données (OCPD)[2],

émet les directives suivantes :

Art. 1 But

[1] Les présentes directives fixent les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir pour obtenir une certification de l'organisation ou de la procédure au sens de l'article 4 OCPD. Elles tiennent compte des normes internationales relatives à l'installation, l'exploitation, la surveillance et l'amélioration de systèmes de gestion et en particulier d'ISO/CEI 27001:2005[3].

[2] Ces directives comprennent intégralement la norme ISO 27001 précitée, qu'elles interprètent au sens de l'article 2 et qu'elles complètent ou amendent au sens de l'article 3 ci-après.

Art. 2 Interprétation

[1] Au sens des présentes directives, il faut comprendre **protection des données (PD)** en lieu et place de *sécurité de l'information (SI)*, en particulier pour les systèmes de gestion (soit **SGPD** pour SGSI).

[2] La notion de **(non-)conformité** relative aux **exigences de protection des données** vient systématiquement compléter celle de *risques* relatifs aux *objectifs de sécurité d'information*.

---

[1] RS **235.1**
[2] RS **……..**
[3] ISO/CEI 27001:2005 « Systèmes de gestion de la sécurité de l'information – Exigences », disponibles sous licence en format papier ou PDF auprès de www.iso.org .

Art. 3 Mise en œuvre

0. Introduction

1. Domaine d'application

   Compatible avec art. 4, al. 1 OCPD.

2. Références normatives

   Loi fédérale sur la protection des données
   (LPD du 19 juin 1992 ; RS 235.1)

   Ordonnance relative à la loi fédérale sur la protection des données
   (OLPD du 14 juin 1993 ; RS 235.11)

   Ordonnance sur les certifications en matière de protection des données
   (OCPD du 28 septembre 2007 ; RS …)

   Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention STE No. 108 / CE du 28.I.1981)

   Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (Protocole STE No. 181 / CE du 8.XI.2001)

3. Termes et définitions

   3.17 Protection des données (art. 1 LPD)
   « Protection de la personnalité et des droits fondamentaux des personnes qui font l'objet d'un traitement de données *personnelles* ».

   3.18 Gestion de la conformité
   Activités coordonnées d'une organisation pour respecter les exigences légales et réglementaires auxquelles elle est soumise, en particulier toutes celles liées à la protection des données.

   3.19 Analyse (appréciation) de non-conformité
   Utilisation systématique d'informations pour identifier les sources de non-conformité et estimer la non-conformité (nature mineure ou majeure).

   3.20 Traitement de non-conformité
   Processus de sélection et implémentation de mesure(s) pour remédier à une non-conformité. A défaut, il est également possible d'éviter une non-conformité, par exemple en renonçant au traitement concerné.

4. Système de gestion

   4.2.1 b) 2) Clause fondamentale.

   4.2.1 d) 1) Porter une attention particulière aux actifs de type **fichiers** (art. 3 let. g LPD) et comprendre **maître de fichier** (art. 3 let. i LPD) pour propriétaire.

   4.2.1 e) 4) Toutes les non-conformités doivent être traitées.

   4.2.1 f) 2) Inapplicable aux non-conformités.

   4.2.1 f) 4) Inapplicable aux non-conformités.

   4.2.1 g) Cf. Guide d'implémentation du SGPD en annexe.

   4.2.1 h) Inapplicable aux non-conformités.

   4.2.3 d) 6) Clause fondamentale.

   4.3.1 j) Nouveau La liste des fichiers non déclarés (cf. mesure 8.2 de l'annexe) !

5. Responsabilité de la Direction

   5.2.1 c) Clause fondamentale.

6. Audits internes du SGPD

   6. a) Clause fondamentale.

7. Revue de Direction du SGPD

   7.3 c) 4-5) Clauses fondamentales.

   7.3 c) 6) Inapplicable aux non-conformités.

8. Amélioration du SGPD

Art. 4 Entrée en vigueur

Les présentes directives entrent en vigueur le … 2008.

Préposé fédéral à la protection des données et à la transparence

Hanspeter Thür

Annexe : Guide d'implémentation des directives pour SGPD
(version préliminaire 0.9 du 30.10.2007)

1. **Licéité** (art. 4, al. 1 LPD)

Objectif du principe: assurer que le *traitement* de données personnelles est entrepris d'une manière licite.

1.1 Motifs justificatifs (art. 13 LPD)

Mesure
Les personnes privées qui 'traitent' (art. 3, let. e LPD) des 'données personnelles' (art. 3, let. a LPD) ont besoin d'un motif justificatif, en d'autres termes, du *consentement* de la 'personne concernée' (art. 3, let. b LPD), d'un *intérêt prépondérant* privé ou public ou d'une *loi*.

Implémentation (art. 4, al. 5 LPD)
Le *consentement* par la 'personne concernée' n'est *valable*, que si elle exprime *librement* sa *volonté,* après avoir été *dûment informée*. Lorsqu'il s'agit de 'données sensibles' (art. 3, let. c LPD) ou de 'profils de la personnalité' (art. 3, let. d LPD), son consentement doit au surplus être *explicite*. Il s'agit en d'autres termes de vérifier l'absence de toutes contraintes directes ou indirectes, ainsi que la pertinence de l'information délivrée. Le consentement est explicite, si la 'personne concernée' a signé de manière autographe ou électronique le document fourni.
Il faut vérifier, le cas échéant, la vraisemblance de l'intérêt prépondérant privé ou public, ou alors l'existence d'une base légale. Il peut s'agir d'une base légale au niveau fédéral (loi au sens formel ou ordonnance ou autre) ou même au niveau cantonal. Le motif justificatif ne vaut que pour le but indiqué par la loi.

1.2 Base légale (art. 17, 19 et 20 LPD)

Mesure
Les organes fédéraux ne sont en droit de traiter des données personnelles que s'il existe une *base légale*; lors du traitement de données sensibles ainsi que de profils de la personnalité, celui-ci doit être expressément prévu dans une base légale *au sens formel* (art. 3, let. j LPD).

Implémentation
Vérifier quel organe fédéral est responsable du traitement de données, ainsi que l'existence d'une base légale, de surcroît 'au sens formel' pour des données sensibles ou des profils de la personnalité.
Vérifier, si la base légale contient tous les éléments nécessaires.
Dans le cas où des données personnelles sont rendues accessibles en ligne, s'assurer que cela est prévu expressément. S'agissant de données sensibles ou de profils de la personnalité, un accès en ligne n'est autorisé que si une loi au sens formel le prévoit expressément.
Concernant les données sensibles ou les profils de la personnalité, dans les cas où il n'y a pas de base légale formelle expresse, il faut vérifier s'il s'agit d'un cas d'exception selon l'art. 17, 2^{e} al. LPD.
Lorsqu'il s'agit d'un traitement de données automatisé dans le cadre d'essais pilotes, il faut vérifier, si les conditions selon l'art. 17a LPD sont remplies.
Pour la communication de données personnelles, ou il n'existe pas de base juridique au sens susmentionné, il doit être vérifié, si une des conditions de l'art. 19 LPD est remplie.

Il faut contrôler, si les instruments nécessaires ont été installés, pour assurer une opposition éventuelle à la communication des données selon l'art. 20 LPD.

Autre information (art. 22 LPD)
Les organes fédéraux sont en droit sous certaines conditions de traiter des données personnelles à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la *recherche*, de la *planification* ou de la *statistique.*

1.3 Traitement de données par un tiers (art. 10a, al. 1 LPD)

Mesure
Le traitement de données peut être *confié à un tiers*, pour autant qu'une *convention* ou la *loi* le prévoie, et que le mandant ait pris les mesures nécessaires pour que seuls les traitements que lui-même serait en droit d'effectuer, sont effectués. En plus, aucune obligation légale ou contractuelle de garder le secret ne doit l'interdire.

Implémentation
Vérifier l'existence d'une convention ou loi prévoyant un traitement par des tiers, ainsi que l'existence des conditions de l'art. 10a LPD. En particulier, vérifier les mesures prises pour assurer que seuls les traitements que le mandant serait en droit d'effectuer lui-même sont effectivement effectués et qu'aucune base légale ou contractuelle de garder le secret ne l'interdise. S'assurer s'il y a lieu de la vraisemblance du motif justificatif.

2. Transparence

Objectif du principe: assurer que le traitement de données personnelles est accompli dans des conditions loyales et transparentes, c'est-à-dire en aucun cas à l'insu de la personne concernée ou pour des finalités détournées.

2.1 Bonne foi (art. 4, al. 2 LPD)

Mesure
Assurer que le traitement de données personnelles est accompli conformément au principe de la bonne foi.

Implémentation
Vérifier que le traitement ne se fait pas de manière secrète, sauf, si une loi le prévoit expressément (dans le domaine de la police par exemple).
Vérifier l'absence de contraintes ou d'éléments trompeurs. S'assurer que la personne concernée a été suffisamment informée de la manière et du but du traitement et qu'elle n'a pas été informée de manière fausse.

2.2 Reconnaissabilité (art. 4, al. 4 LPD)

Mesure
Assurer que la *collecte* de données personnelles, et en particulier les *finalités du traitement*, sont reconnaissables pour la personne concernée.

Implémentation
Vérifier que les informations concrètes à disposition de la personne concernée suffisent à assurer la reconnaissabilité.

2.3 Obligation d'informer (art. 7a, al. 1 LPD)

Mesure
Le *maître du fichier* (art. 3, let. i LPD) a l'obligation d'informer la personne concernée lorsqu'il collecte des données sensibles ou des profils de la personnalité la concernant, que la collecte soit effectuée directement auprès d'elle ou auprès d'un tiers.

Implémentation (art. 7a, al. 2 LPD)
La personne concernée doit au minimum recevoir les informations suivantes:
a. l'identité du maître du fichier;
b. les finalités du traitement pour lequel les données sont collectées;
c. les catégories de destinataires des données si la communication des données est envisagée.

3. Proportionnalité

Objectif du principe : assurer que le traitement de données personnelles est proportionnel, c'est-à-dire *apte* à atteindre le but ou accomplir la tâche, *nécessaire* à ce dessein et *raisonnable* par rapport à l'atteinte qu'il implique pour la personne concernée.

3.1 Traitement proportionnel (art. 4, al. 2 LPD)

Mesure
Ne peuvent être traitées que les données absolument utiles et nécessaires (*évitement* et/ou *minimisation* de données) à l'accomplissement de la tâche ou à l'atteinte du but. Les *données sensibles* doivent à cet égard faire l'objet d'une attention toute particulière. Les données personnelles inutiles doivent être détruites ou alors anonymisées, à moins qu'il existe des obligations d'archivage ou de conservation. Dans les cas ou l'identité de la personne n'est pas nécessaire, le traitement doit se faire sous forme pseudonymisée.

Implémentation
L'*anonymisation* de données personnelles consiste en une *élimination* de tous les éléments permettant une identification, de sorte que les données ne soient plus du tout corrélables à une personne identifiée ou identifiable (donc même plus soumises à la LPD).
La *pseudonymisation* de données personnelles consiste en un *remplacement* de tous les éléments permettant une identification par un identifiant neutre appelé *pseudonyme*, ce dernier étant parallèlement mémorisé avec les éléments d'identification dans une *table annexe de correspondance* permettant aux ayants droit d'établir au besoin le lien avec la personne concernée (identifiabilité au sens de la LPD). L'avantage stratégique ainsi obtenu est que les données pseudonymisées peuvent être considérées comme "anonymes" pour l'ensemble des personnes n'ayant aucun accès à la table de correspondance. Une telle démarche n'a de sens, que si la *table de correspondance* jouit d'une *protection exemplaire*, soit n'est gérée que par des personnes autorisées et authentifiées, n'est mémorisée que sous une forme chiffrée et n'autorise en principe qu'une réidentification individuelle avec journalisation exhaustive des « dépseudonymisations » effectuées.
En ce qui concerne les *données biométriques* issues de la *capture* de caractéristiques physiologiques humaines comme l'empreinte digitale, la main, le visage, l'iris ou même

l'empreinte génétique, ou alors de caractéristiques comportementales comme la signature, la voix ou la frappe au clavier, le rapport entre la finalité du traitement et l'atteinte aux personnes concernées doit rester raisonnable. Cette appréciation doit en particulier tenir compte du *caractère unique et irremplaçable* des données biométriques, ainsi que de leur *nature primaire* (données brutes ou crues) *ou secondaire* (données dérivées ; gabarits). En principe, on favorisera toujours l'utilisation de caractéristiques biométriques *ne laissant pas de traces physiques* (ex. contour de la main), la *décentralisation* des données biométriques (en seule possession des personnes concernées) et/ou le recours à des *gabarits biométriques* (moins intrusifs que les données primaires correspondantes).

4. **Finalité** (art. 4, al. 3 LPD)

Objectif du principe : assurer que les données personnelles ne sont traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances.

4.1 Spécification/Modification de la finalité (art. 3, let. i LPD)

Mesure
Le 'maître du fichier' doit consigner le but du 'traitement' dans un document ad hoc.

Implémentation
La finalité du traitement doit être décrite dans un document spécifique et concis, écrit dans un langage clair et facilement compréhensible par les personnes concernées. Ce document doit être daté et signé par le 'maître de fichier'.
Toute modification subséquente de la finalité initiale doit pouvoir être reconstituée, tout comme les actions informationnelles (publication officielle, nouveaux consentements, etc.) entreprises vis-à-vis des personnes concernées.

4.2 Limitation d'utilisation

Mesure
Assurer que le 'traitement' de 'données personnelles' reste dans le cadre du but défini.

Implémentation
Tout traitement de données qui va au-delà des buts spécifiés initialement représente un **détournement de finalité** qui peut être dénoncé et sanctionné.

Autre information (art. 10, al. 1 OLPD)
Le maître du fichier *journalise* les traitements automatisés de données sensibles ou de profils de la personnalité lorsque les mesures préventives ne suffisent pas à garantir la protection des données. Une journalisation est notamment nécessaire, lorsque, sans cette mesure, il ne serait *pas possible de vérifier a posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées* ou communiquées. Le préposé peut recommander la journalisation pour d'autres traitements.

5. Exactitude des données

Objectif du principe : assurer que les 'données personnelles' traitées sont et restent exactes.

5.1 Exactitude des données (art. 5, al. 1 LPD)

Mesure
Assurer que les 'données personnelles' traitées sont correctes et prendre toute mesure appropriée permettant d'effacer ou de rectifier les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées.

Implémentation
Lorsque des données personnelles sont collectées, il faut prendre des mesures raisonnables pour *authentifier* la personne concernée et valider la *plausibilité* des informations reçues. Des contraintes adéquates (formats prédéfinis, etc.) dans les masques permettent d'éviter de nombreuses fautes de frappe ou autres mauvaises saisies.
Une donnée personnelle dont l'exactitude ne peut être garantie ne doit pas être collectée ou alors nécessairement être révisée ou détruite après un certain temps prédéfini. Des solutions cryptographiques pourraient empêcher tout déchiffrement après une date de péremption.
La mise à jour des données collectées doit être assurée par le maître de fichier.

5.2 Rectification des données (art. 5, al. 2 LPD)

Mesure
Toute 'personne concernée' peut requérir la rectification des données inexactes.

Implémentation
En exerçant son droit d'accès ou ayant un accès direct de lecture sur ses propres données, une personne concernée peut découvrir que des données inexactes ont été collectées et/ou sont traitées par le maître de fichier. L'art. 15 lui permet alors de demander que ces données soient rectifiées ou détruites ou que la transmission de celles-ci soit interrompue. Si l'inexactitude des données ne peut être établie, le requérant peut demander leur marquage par mention de leur nature litigieuse.

6. Communication transfrontière de données (art. 6, al. 1 LPD)

Objectif du principe: aucune 'donnée personnelle' ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une législation assurant un niveau de protection adéquat.

6.1 Niveau de protection adéquat (art. 6, al. 2 LPD)

Mesure
En dépit de l'absence d'une législation assurant un niveau de protection adéquat à l'étranger, des données personnelles peuvent être communiquées à l'étranger, à l'une des conditions suivantes uniquement:

a. des *garanties suffisantes*, notamment contractuelles, permettent d'assurer un niveau de protection adéquat à l'étranger;
b. la personne concernée a, en l'espèce, *donné son consentement*;

c. le traitement est en *relation directe avec la conclusion ou l'exécution d'un contrat* et les données traitées concernent le cocontractant;
d. la communication est, en l'espèce, indispensable *soit à la sauvegarde d'un intérêt public prépondérant*, soit à la constatation, l'exercice ou la défense d'un droit en justice;
e. la communication est, en l'espèce, *nécessaire pour protéger la vie ou l'intégrité corporelle* de la personne concernée;
f. la personne concernée a rendu *les données accessibles à tout un chacun* et elle ne s'est pas opposée formellement au traitement;
g. la communication a lieu *au sein d'une même personne morale ou société* ou entre des personnes morales ou sociétés réunies sous une direction unique, dans la mesure où les parties sont soumises à des règles de protection des données qui garantissent un niveau de protection adéquat.

Implémentation (art. 6, al. 1 LPD)
Vérifier que les destinataires de données sont soumis à une législation assurant un niveau de protection adéquat (cf. Liste indicative des États ayant une législation assurant un niveau de protection de données adéquat au regard du droit suisse, publiée sur www.leprepose.ch), ainsi que la qualité des garanties fournies pour les points a et g.

7. **Sécurité des données** (art. 7 LPD)

Objectif du principe: assurer que les 'données personnelles' sont protégées contre tout 'traitement' non autorisé par des mesures techniques et organisationnelles appropriées.

7.1 Confidentialité des données

Mesure
Assurer que les 'données personnelles' ne sont pas mises à disposition ou révélées à des individus, entités ou processus non autorisés.

Implémentation (Annexe A d'ISO 27001, renvoyant intégralement à ISO 27002)

A.7.x	Gestion des actifs
A.10.6.x	Gestion de la sécurité des réseaux
A.10.7.x	Manipulation des supports
A.10.8.x	Échange des informations
A.10.10.x	Surveillance
A.11.x	Contrôle d'accès

Le contrôle 7.2 porte sur la *classification* des informations : le niveau de protection des données traitées peut être évalué selon leur degré de sensibilité. Une classification de protection des données doit au minimum faire la différence entre un « *niveau normal* » de protection pour des données personnelles dont l'usage abusif ne pourrait causer qu'un dommage mineur à la personne concernée, et un « *niveau élevé* » de protection pour des données personnelles sensibles ou des profils de personnalité, dont l'usage abusif pourrait lui causer un dommage majeur voire représenter un danger pour sa vie. Tout niveau intermédiaire de protection entre ces deux peut être défini, mais il est recommandé de ne pas dépasser un total de 4 niveaux de protection.

7.2 Intégrité des données

Mesure
Assurer la complétude, la validité et l'actualité des données personnelles.

Implémentation
A.10.4.x Protection contre les codes malveillant et mobile
A.12.x Acquisition, développement et maintenance des systèmes d'information

7.3 Disponibilité des données

Mesure
Assurer que les 'données personnelles' sont accessibles et exploitables sur demande par une entité autorisée.

Implémentation
A.10.5.1 Sauvegarde des informations
A.14.x Gestion du plan de continuité de l'activité (SGCA)
A.15.1.3 Protection des enregistrements de l'organisme

7.4 Traitement de données par un tiers (art 10a, al. 2 LPD)

Mesure
Le mandant doit en particulier s'assurer que le *tiers garantit la sécurité des données*.

Implémentation
Vérifier la qualité des instructions données au mandataire par le mandat, afin de voir si elles répondent aux exigences attendues (cf. mesures ci-dessus).

8. **Enregistrement des fichiers** (art. 11a, al. 1 LPD)

Objectif du principe: le préposé tient un *registre des fichiers accessible en ligne*. Toute personne peut consulter ce registre.

8.1 Obligation de déclarer (art. 11a, al. 2 et 3 LPD; exceptions art. 11a, al. 5, let. f-e LPD)

Mesure
Les organes fédéraux sont tenus de déclarer tous leurs 'fichiers' au PFPDT, tandis que les personnes privées doivent déclarer leurs fichiers, si elles traitent régulièrement des données sensibles ou des profils de la personnalité, ou si elles communiquent régulièrement des données personnelles à des tiers.
Les fichiers ne doivent par contre pas être déclarés lorsqu'une *certification a été obtenue* pour l'ensemble des procédures de traitement portant sur les données du fichier à déclarer et que le résultat de l'audit a été communiqué au PFPDT, ou lorsqu'un *conseiller indépendant à la protection des données a été désigné*.

Implémentation
Le PFPDT mettra sous peu à disposition des organes fédéraux comme des personnes privées une nouvelle application WebDatareg qui permettra la déclaration et la mise à jour en ligne des fichiers concernés. Toutes les consignes et prescriptions de déclaration seront également

fournies en ligne. À terme, WebDatareg permettra au public de consulter sur Internet les informations du registre des fichiers annoncés, afin de pouvoir s'adresser à la personne qui pourra la renseigner ou auprès de laquelle elle pourra faire valoir son droit d'accès.

8.2 Inventaire des fichiers non déclarés (art. 12b, al. 1, let. b OLPD)

Mesure
Le maître des fichiers prend toutes les mesures nécessaires, afin de pouvoir communiquer sur demande au préposé ou aux personnes concernées les informations concernant les fichiers non soumis à la déclaration.

Implémentation
Assurer la mise en place des mesures nécessaires afin de pouvoir communiquer sur demande au préposé ou aux personnes concernées les informations concernant les fichiers non soumis à la déclaration et afin de pouvoir tenir le fichier à jour.
Établir et gérer un inventaire des fichiers non déclarés contenant les informations suivantes :

a. les nom et adresse du maître du fichier ;
b. le nom et la dénomination complète du fichier ;
c. la personne auprès de laquelle peut être exercé le droit d'accès ;
d. le but du fichier ;
e. les catégories de données personnelles traitées ; les catégories de destinatiares des données ;
f. les catégories de participants au ficher, c'est-à-dire les tiers qui sont en droit d'introduire des données dans le fichier ou d'y procéder à des mutations.

9. Droit d'accès et de procédure

Objectif du principe: toute personne peut demander au maître d'un fichier si des données la concernant sont traitées. S'il y a un traitement illicite, la personne concernée peut demander que les données soient rectifiées, détruites ou bloquées (interdites de communication à des tiers).

9.1 Droit d'accès à ses propres données (art. 8, al. 1 LPD)

Mesure
Toute personne peut demander au maître d'un fichier si des données la concernant sont traitées.

Implémentation (art. 8, al. 2 et 3 LPD)
Le maître du fichier doit communiquer toutes les données concernant le demandeur qui sont contenues dans le fichier, le but et éventuellement la base juridique du traitement, les catégories de données personnelles traitées, de participants au fichier et de destinataires de données. Il peut communiquer à la personne concernée des *données sur sa santé* par l'intermédiaire d'un médecin qu'elle a désigné.
Pour permettre de vérifier l'exécutabilité de ce droit, les applications devraient comprendre (dans leur menu) une **routine prédéfinie de droit d'accès** fournissant d'une manière claire toutes les données relatives à une personne identifiée.

Autres informations (art. 9 et 10 LPD)
Le droit d'accès ne peut être *refusé*, *restreint* ou *différé* que dans les cas prévus par la loi.

Le maître de fichier doit alors indiquer le motif pour lequel il refuse de fournir, limite ou ajourne les renseignements.
Le maître d'un fichier utilisé exclusivement pour la publication dans la partie rédactionnelle d'un média à caractère périodique peut sous certaines conditions refuser ou restreindre la communication des renseignements demandés, voire en différer l'octroi.

9.2 Prétentions et procédures (art. 15, al. 1 et 2 LPD)

Mesure
S'il y a un traitement illicite, la personne concernée peut demander que les données soient *rectifiées*, *détruites* ou *bloquées* (interdites de communication à des tiers). Si ni l'exactitude, ni l'inexactitude d'une donnée personnelle ne peut être établie, le demandeur peut requérir que l'on ajoute la *mention de son caractère litigieux*.

Implémentation (art. 15, al. 4 LPD)
Vérifier les instruments et processus mis en place pour l'exercice du droit de rectification, de destruction, de blocage ou de mention. Avec l'introduction du devoir d'information (art. 7a), le droit de requérir l'interdiction du traitement des données est devenu plus effectif.
Il faut contrôler, si les instruments nécessaires ont été installés, pour assurer une opposition éventuelle à la communication des données selon l'art. 20 LPD.