Annexe des directives sur les exigences minimales qu'un SGPD doit remplir (Version du 15.04.2014)

Table de matière

Code de bonne pratique pour la gestion de la protection des données:

Ce code de bonne pratique pour la gestion de la protection des données (CBPGPD) est subdivisé logiquement selon 9 principes généraux de la loi fédérale sur la protection des données (LPD; RS 235.1) et concrétise le point 5 des « Directives sur les exigences minimales qu'un système de gestion de protection des données (SGPD) doit remplir ». Il reprend de manière non exhaustive[1] les exigences principales de la LPD et de son ordonnance d'application (OLPD; RS 235.11). Selon le domaine d'utilisation (santé, télécommunication, statistique, etc.), les dispositions légales spéciales en matière de protection des données doivent en outre être prises en compte. Afin d'en faciliter la lecture et la compréhension, chaque mesure est structurée de manière analogue au « Code de bonne pratique pour la gestion de la sécurité de l'information (ISO/CEI 27002:2013[2]) », qui sert par ailleurs de référence aux mesures portant sur la sécurité des données (principe numéro 7). À la différence d'ISO 27002 qui se base sur une analyse de risques, les mesures du CBPGPD sont formulées de manière impérative (doit, nécessite, requiert, faut, etc.), du fait qu'elles font suite à une analyse de non-conformité et qu'elles découlent directement de la LPD ou de l'OLPD.

a. Licéité (art. 4, al. 1, LPD)

Objectif

Assurer que le *traitement* de données personnelles est entrepris d'une manière licite.

a.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*.

Mise en œuvre (art. 4, al. 5, LPD)

Le *consentement* de la 'personne concernée' (art. 3, let. b, LPD) n'est *valable*, que si elle exprime *librement* sa *volonté,* après avoir été *dûment informée*. En d'autres termes, le consentement doit être accordé en l'absence de toute contrainte directe ou indirecte, et sur la base d'une information objective et pertinente. Pour des 'données sensibles' (art. 3, let. c, LPD) ou des 'profils de la personnalité' (art. 3, let. d, LPD), le consentement doit au surplus être *explicite*. Le consentement est explicite, si la 'personne concernée' a signé de manière autographe ou électronique le document informatif reçu.

Le cas échéant, la vraisemblance de l'intérêt prépondérant privé ou public, ou l'existence d'une base légale doit pouvoir être établie. Il peut s'agir d'une base légale au niveau fédéral (loi au sens formel, ordonnance ou autre) ou au niveau cantonal. Le motif justificatif ne vaut que pour le but indiqué par la loi.

---

[1] Les brochures et guides du PFPDT, ainsi que les explications et FAQ de l'OFJ, peuvent apporter des éclairages et informations utiles pour concrétiser les objectifs et mesures énumérés dans ce code de bonne pratique.

[2] Modification du 15.04.2014

a.2 Base légale (art. 17, 19 et 20 LPD)

Mesure

Les 'organes fédéraux' (art. 3, let. h, LPD) ne sont en droit de traiter des données personnelles que s'il existe une *base légale*; le traitement de données sensibles et de profils de la personnalité doit être expressément prévu par une 'loi au sens formel' (art. 3, let. j, LPD).

Mise en œuvre

- L'organe fédéral responsable du traitement de données doit pouvoir être identifié.
- Une base légale, de surcroît 'au sens formel' pour des données sensibles ou des profils de la personnalité, doit exister. Celle-ci doit contenir tous les éléments nécessaires, en particulier l'organe responsable et le but du traitement, les catégories de données traitées, de destinataires et/ou de participants.
- En l'absence de cette base légale, il doit s'agir d'une exception prévue à l'art. 17, al. 2, let. a-c ou à l'art. 19, al. 1-2, LPD.
- Des données personnelles ne peuvent être rendues accessibles en ligne, que si cela est prévu expressément. S'agissant de données sensibles ou de profils de la personnalité, l'accès en ligne n'est autorisé que si une loi au sens formel le prévoit expressément.
- Les organes fédéraux peuvent rendre accessibles des données personnelles à tout un chacun au moyen de services d'information et de communication automatisés, lorsqu'une base juridique prévoit la publication de ces données ou lorsque ces organes rendent des informations accessibles au public sur la base de l'art. 19, al. 1bis, LPD.
- En cas d'un traitement de données automatisé dans le cadre d'essais pilotes, les conditions prévues à l'art. 17*a* LPD doivent être remplies.
- Les instruments permettant de s'opposer à la 'communication' (art. 3, let. f, LPD) des données selon l'art. 20 LPD doivent exister et pouvoir être utilisés.

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.*

a.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 les conditions suivantes soient remplies:

- seuls les traitements que le mandant serait en droit d'effectuer lui-même sont effectués;
- aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

Mise en œuvre

- Une convention ou la loi doit prévoir le traitement par des tiers et les conditions prévues à l'art. 10*a* LPD doivent être remplies.
- Un tiers a l'interdiction d'effectuer d'autres traitements que ceux que le mandant serait lui-même en droit d'effectuer, donc chacun des traitements effectués par un tiers doit être licite pour le mandant.
- S'assurer formellement qu'aucune base légale ou contractuelle de garder le secret n'interdise le traitement.
- S'il y a lieu, la vraisemblance du motif justificatif doit pouvoir être établie.

- Le contrôle A.15.1 « Sécurité dans les relations avec les fournisseurs » de l'annexe A de la norme ISO/CEI 27001:2013 ("Exigences pour SMSI") s'applique à titre complémentaire[3].

Autre information[4]

Cf. mesure g.4 pour la garantie de la sécurité des données dans le cadre du traitement de données par un tiers.

b. Transparence

Objectif

Assurer que le traitement de données personnelles est accompli dans des conditions loyales et transparentes, c'est-à-dire n'intervient pas à l'insu de la personne concernée ou pour des finalités détournées.

b.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.

Mise en œuvre

- Le traitement ne doit pas être accompli à l'insu de la personne concernée, sauf si une loi le prévoit expressément (dans le domaine de la police par exemple).
- Le traitement doit avoir lieu en l'absence de contraintes ou d'éléments trompeurs.
- La personne concernée doit être suffisamment et correctement informée de la méthode et du but du traitement.

b.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.

Mise en œuvre

Les informations concrètes à disposition de la personne concernée doivent suffire à assurer la reconnaissabilité de la collecte des données et des finalités de leur traitement.

b.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.

---

[3] Modification du 15.04.2014

[4] Modification du 15.04.2014

Mise en œuvre (art. 7*a*, al. 2-3, LPD)

- Le 'maître du fichier' doit transmettre à la 'personne concernée' au minimum les informations suivantes:
  - son identité (maître du fichier);
  - les finalités du traitement pour lequel les données sont collectées;
  - les catégories de destinataires des données si la communication des données est envisagée.
- Si les données ne sont pas collectées auprès de la personne concernée, le maître du fichier doit l'informer au plus tard lors de leur enregistrement ou, en l'absence d'un enregistrement, lors de leur première communication à un tiers.

Autre information (art. 7a, al. 4, LPD)

Le maître du fichier est délié de son devoir d'information si la personne concernée a déjà été informée; il n'est pas non plus tenu d'informer cette dernière, quand les données ne sont pas collectées directement auprès d'elle, si:

- l'enregistrement ou la communication sont expressément prévus par la loi;
- le devoir d'information est impossible à respecter ou nécessite des efforts disproportionnés.

c. Proportionnalité

Objectif

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.

c.1 Traitement proportionnel (art. 4, al. 2, LPD)

Mesure

Ne doivent être traitées que les données absolument utiles et nécessaires (*évitement* 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, sauf obligation d'archivage ou de conservation.

Dans les cas où l'identité de la personne n'est pas nécessaire, le traitement doit se faire sous forme pseudonymisée ou anonymisée.

Mise en œuvre

- 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 ou alors au prix d'efforts démesurés[5] corrélables à une personne identifiée ou identifiable (elles ne sont dès lors 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 de correspondance annexe* permettant aux ayants droit d'établir au besoin le lien avec la personne concernée (identifiabilité au sens de la LPD). Cette méthode présente l'avantage

[5] Ajout du 10.03.2010

que les données pseudonymisées peuvent être considérées comme "anonymes" pour quiconque n'a pas accès à la table de correspondance. Cette démarche n'a de sens que si la *table de correspondance* jouit d'une *protection exemplaire*, qu'elle n'est gérée que par des personnes autorisées et authentifiées, qu'elle n'est mémorisée que sous une forme chiffrée et qu'elle ne permet 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 l'empreinte génétique, ou 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). On favorisera l'utilisation de caractéristiques biométriques *ne laissant pas de traces physiques* (ex. contour de la main), le recours à des *données biométriques secondaires* (*gabarits biométriques* en principe moins intrusifs que les données primaires correspondantes) et, dans le cadre d'une finalité de vérification, la *décentralisation* des données biométriques (en seule possession des personnes concernées).

d. Finalité (art. 4, al. 3, LPD)

Objectif

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.

d.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 idoine.

Mise en œuvre

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

d.2 Limitation de l'utilisation

Mesure

Assurer que le 'traitement' de 'données personnelles' ne s'écarte pas du but défini.

Tout traitement de données allant au-delà des buts fixés au moment de la collecte constitue un **détournement de finalité** qui peut être dénoncé et sanctionné.

Mise en œuvre (art. 10 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. La 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.

- Les fichiers journaux sont *conservés durant une année* et sous une forme répondant aux exigences de la révision. Ils sont accessibles aux seuls organes ou personnes chargés de vérifier l'application des dispositions de protection des données, et ils ne sont *utilisés qu'à cette fin*.

e. Exactitude des données

Objectif

Assurer que les 'données personnelles' traitées sont et restent exactes.

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

Mesure

Celui qui traite des 'données personnelles' doit s'assurer qu'elles 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 traitées.

Mise en œuvre

- 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 de saisie.
- Une donnée personnelle dont l'exactitude ne peut être assurée par des mesures raisonnables ne doit pas être collectée ou sera nécessairement révisée ou détruite après un certain laps de temps. Des solutions cryptographiques peuvent empêcher tout déchiffrement des données après leur date de péremption.
- Le maître de fichier doit assurer la mise à jour des données collectées.

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

Mesure

Celui qui traite des données personnelles doit assurer la rectification des données inexactes, notamment sur requête de la personne concernée.

Mise en œuvre

En exerçant son droit d'accès ou en accédant directement (en mode lecture) à ses propres données, la personne concernée peut découvrir que des données inexactes ont été collectées ou sont traitées par le maître de fichier. L'art. 15 ou 25 LPD lui permet de demander que ces données soient rectifiées ou détruites ou que la transmission de celles-ci soit interrompue. Si ni l'exactitude, ni l'inexactitude des données ne peut être établie, le requérant peut demander leur marquage par mention de leur nature litigieuse. Il incombe au maître du fichier de mettre en place les outils permettant la rectification, la destruction ou le marquage des données, de même que l'interruption de leur transmission s'il y a lieu.

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

Objectif

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.

f.1 Niveau de protection adéquat (art. 6, al. 2, LPD)

Mesure

La communication de données personnelles ne doit représenter aucune grave menace de la personnalité des personnes concernées. À noter qu’une telle menace est présumée, lorsque les destinataires de données ne sont pas soumis à une législation assurant un niveau de protection adéquat.

Mise en œuvre (art. 6, al. 1, LPD)

L’État destinataire doit faire partie de la 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).

En l’absence d’une législation assurant un niveau de protection adéquat à l’étranger, une des garanties suivantes doit exister:

- **garanties suffisantes**, notamment contractuelles, permettant d’assurer un niveau de protection adéquat à l’étranger (art. 6, al. 2, let. a, LPD);
- garantie que les parties sont soumises à des **règles de protection des données** qui garantissent un niveau de protection adéquat, lorsque 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 (art. 6, al. 2, let. g, LPD).

À défaut d’une des garanties ci-dessus, une des conditions suivantes doit être remplie:

- la personne concernée a en l’espèce donné son consentement (art. 6, al. 2, let. b, LPD);
- le traitement est en relation directe avec la conclusion ou l’exécution d’un contrat et les données traitées concernent le cocontractant (art. 6, al. 2, let. c, LPD);
- 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 (art. 6, al. 2, let. d, LPD);
- la communication est, en l’espèce, nécessaire pour protéger la vie ou l’intégrité corporelle de la personne concernée (art. 6, al. 2, let. e, LPD);
- la personne concernée a rendu les données accessibles à tout un chacun et elle ne s’est pas opposée formellement au traitement (art. 6, al. 2, let. f, LPD);

g. Sécurité des données (art. 7 LPD)

Objectif

Assurer que les ‘données personnelles’ sont protégées contre tout ‘traitement’ non autorisé par des mesures techniques et organisationnelles appropriées.

g.1 Confidentialité des données

Mesure

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

Mise en œuvre[6] (Annexe A d'ISO 27001, renvoyant intégralement à ISO 27002)

A.6.1.5[nouv]	Sécurité de l'information dans la gestion de projet (=> "Privacy by Design")
A.6.2[nouv]	Appareils mobiles et télétravail
A.8.x	Gestion des actifs
A.9.x	Contrôle d'accès
A.10.x[nouv]	Cryptographie
A.11.x[7]	Sécurité physique et environnementale
A.12.4	Journalisation et surveillance
A.13.1	Gestion de la sécurité des réseaux
A.13.2	Transfert de l'information

Le contrôle A.8.2 porte sur la *classification* des informations: le niveau de protection des données traitées peut être évalué selon leur degré de sensibilité. La classification de protection des données doit au minimum distinguer le « *niveau normal* » de protection pour les données personnelles dont l'usage abusif ne pourrait causer qu'un dommage mineur à la personne concernée du « *niveau élevé* » de protection pour les données personnelles sensibles ou les profils de personnalité, dont l'usage abusif pourrait causer un dommage majeur à la personne concernée voire mettre sa vie en danger. Il est possible de définir des niveaux intermédiaires, mais il est recommandé de ne pas prévoir plus de quatre niveaux de protection.

g.2 Intégrité des données

Mesure

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

Mise en œuvre[8]

A.12.2	Protection contre les logiciels malveillants
A.14.x	Acquisition, développement et maintenance des systèmes d'information

g.3 Disponibilité des données

Mesure

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

Mise en œuvre[9]

A.12.3	Sauvegarde (des informations)
A.17.x	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
A.18.1.3	Protection des enregistrements

[6] Modification du 15.04.2014

[7] Ajout du 10.03.2010

[8] Modification du 15.04.2014

[9] Modification du 15.04.2014

g.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*.

Mise en œuvre

La qualité des instructions fournies au mandataire par le mandat pour garantir la sécurité des données doit répondre aux exigences attendues (cf. mesures ci-dessus).

Le contrôle A.15.2 « Gestion de la prestation du service » de l'annexe A d'ISO 27001 s'applique à titre complémentaire[10].

Autre information[11]

Cf. mesure a.3 pour les exigences légales dans le cadre du traitement de données par un tiers.

h. Enregistrement des fichiers (art. 11*a*, al. 1, LPD et art. 12*b*, al. 1, OLPD)

Objectif

Assurer la transparence de l'existence des fichiers de données personnelles, afin de faciliter l'exercice de leurs droits par les personnes concernées. Le PFPDT tient à cet effet un *registre des fichiers accessible en ligne*, registre que toute personne peut consulter. Accessoirement, ce registre permet au PFPDT d'avoir un aperçu des fichiers nationaux existants et nouvellement créés, ce qui facilite son activité de surveillance en la matière.

h.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' (art. 3, let. g, LPD) au PFPDT, tandis que les personnes privées ne doivent les déclarer, que si elles traitent régulièrement des données sensibles ou des profils de la personnalité ou qu'elles communiquent régulièrement des données personnelles à des tiers.

Les fichiers peuvent ne 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 alors lorsqu'un *conseiller indépendant à la protection des données a été désigné*.

Mise en œuvre

Le PFPDT met à disposition des organes fédéraux et des personnes privées une nouvelle application WebDatareg qui permet la déclaration et la mise à jour en ligne des fichiers concernés. WebDatareg permet en outre au public d'accéder en ligne aux informations du *registre des fichiers déclarés* et de s'adresser à la personne qui pourra le renseigner ou auprès de laquelle il pourra faire valoir son droit d'accès.

[10] Modification du 15.04.2014

[11] Modification du 15.04.2014

h.2 Inventaire des fichiers non déclarés (art. 12b, al. 1, let. b, OLPD)

Mesure

Un maître de fichiers délié de ses obligations de déclaration doit prendre les mesures nécessaires pour communiquer sur demande au préposé ou aux personnes concernées les informations concernant les fichiers non soumis à la déclaration.

Mise en œuvre

Il faut prendre les mesures nécessaires pour communiquer sur demande au préposé ou aux personnes concernées les informations concernant les fichiers non soumis à la déclaration et tenir le fichier à jour. À cette fin, il faut 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;
f. les catégories de destinataires des données;
g. les catégories de participants au ficher, c'est-à-dire les tiers qui sont en droit de saisir et de modifier des données dans le fichier.

Autre information (Art. 28, al. 3, OLPD)

Le PFPDT tient une *liste des maîtres de fichiers* qui sont déliés du devoir de déclarer leurs fichiers en vertu de l'art. 11*a*, al. 5, let. e, LPD (désignation d'un conseiller indépendant à la protection des données) et let. f (obtention d'un label de qualité après s'être soumis à une procédure de certification), LPD. Cette liste est accessible en ligne, afin que le public puisse anticiper le fait que les fichiers de ces maîtres ne sont en principe pas déclarés dans le registre des fichiers tenu par le PFPDT.

i. Droit d'accès et de procédure

Objectif

Le maître d'un fichier doit répondre à toute personne qui lui demande si des données la concernant y 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).

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

Mesure

Le maître d'un fichier doit répondre à toute personne qui lui demande si des données la concernant y sont traitées.

Mise en œuvre (art. 8, al. 2 et 3, art. 9 et 10, LPD)

Le maître du fichier doit organiser son fichier de façon à permettre l'exercice du droit d'accès. Il doit également mettre en place des outils de recherche permettant de retrouver toutes les données traitées concernant la personne faisant valoir son droit d'accès. Le maître du fichier doit enfin être en mesure de soumettre les informations à la personne concernée.

Le maître du fichier doit communiquer toutes les données concernant le demandeur qui sont contenues dans le fichier, le but et éventuellement la base légale 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 vérifier le caractère exécutable et reproductible du droit d'accès, les applications informatiques doivent comprendre (dans leur menu) une **routine prédéfinie** fournissant de manière claire toutes les données relatives à une personne identifiée.

Le maître du fichier doit mettre sur pied des processus lui permettant de garantir les droits des personnes concernées. 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.

En cas d'ajournement de l'accès, le maître du fichier doit se doter d'un système de rappel. La traçabilité, notamment des éventuels refus et restrictions d'accès, doit également être garantie.

Autre information (art. 10 LPD)

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.

i.2 Prétentions et procédures (art. 15 et 25 LPD)

Mesure

Dans le cadre des réglementations sur les prétentions et procédures, la personne concernée peut demander au juge civil (traitement par des personnes privées) ou au Tribunal administratif fédéral (traitement par des organes fédéraux) 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 à la donnée la *mention de son caractère litigieux*.

Mise en œuvre (art. 15/25, al. 4, LPD)

Les instruments et processus doivent être mis en place pour l'exercice du droit de rectification, de destruction, de blocage ou de mention. Des instruments permettant de s'opposer à la communication des données selon l'art. 20 LPD (traitement de données personnelles par des organes fédéraux) doivent exister et pouvoir être mis en œuvre.

Autre information

L'inscription du devoir d'information dans la loi (art. 7*a* LPD) a renforcé le droit de requérir l'interdiction du traitement des données.