Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Guide pour le traitement des données personnelles dans le secteur privé

Août 2009

Feldeggweg 1, 3003 Berne
Tél. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Table des matières

1. La protection des données dans le secteur privé

La loi fédérale sur la protection des données (LPD) et l'ordonnance relative à la loi fédérale sur la protection des données (OLPD) sont entrées en vigueur le 1er juillet 1993. Leur révision est entrée en force le 1er janvier 2008. Depuis lors, tout traitement de données personnelles doit satisfaire aux exigences de cette loi. Une responsabilité particulière incombe aux «maîtres de fichier», terme qui désigne la personne qui décide du but et du contenu du fichier.

La présente brochure s'adresse aux responsables de fichiers dans le secteur privé. Une autre brochure, relative au traitement des données au sein de l'administration fédérale, est disponible sur le site du Préposé fédéral à la protection des données et à la transparence (PFPDT). Le traitement de données par les administrations cantonales et communales est régi par le droit cantonal.

Cette brochure présente les principes de protection des données qu'un maître de fichier doit respecter, ainsi que les questions qu'il doit se poser avant de collecter, de traiter ou de transmettre des données.

Certains fichiers, ainsi que le transfert de certaines données, doivent être déclarés au Préposé fédéral à la protection des données. Dans les pages qui suivent, vous trouverez donc également les cas dans lesquels le maître de fichier doit préalablement déclarer les fichiers qu'il a décidé d'ouvrir.

Pour toutes questions relatives à la responsabilité des maîtres de fichier ou à la loi sur la protection des données d'une façon générale, veuillez prendre contact avec nous. Vous trouverez notre adresse à la fin de cette brochure.

2. Le maître du fichier et sa responsabilité

Par «maître du fichier», on entend la personne privée – physique ou morale – qui décide du but et du contenu du fichier. Du point de vue de la protection des données, le maître du fichier et la personne qui saisit ou modifie les données peuvent être deux personnes différentes.

2.1 Traitement de données: principes généraux

Les principes qui suivent, et qui sont énoncés aux art. 4 et 5 LPD, doivent impérativement être respectés dans toute opération de traitement de données.

Les données personnelles ne peuvent être collectées que de manière **licite**. On considère que des données ont été collectées de façon illicite lorsqu'elles ont été obtenues par la force, par la ruse, par la menace ou par la tromperie.

Selon la LPD, les données personnelles doivent être traitées en conformité avec le principe de la **bonne foi**; cela signifie que le traitement de données a été effectué de manière reconnaissable pour la personne concernée. Il y a non-respect de ce principe lorsqu'une personne n'a pas été informée – ou a été informée de façon erronée – du type et du but du traitement. Sont notamment considérées comme tromperies intentionnelles les collectes secrètes de données, les écoutes téléphoniques non autorisées, ou encore les collectes de données à l'insu de l'intéressé par la manipulation de programmes.

Les données personnelles ne peuvent être traitées que dans le but qui est indiqué lors de la collecte, qui est prévu par une loi ou qui ressort des circonstances. Ainsi, les adresses recueillies par exemple dans le cadre d'un concours ne peuvent être utilisées à d'autres fins commerciales.

Si vous souhaitez modifier le but du traitement, vous devez obtenir l'accord exprès des personnes concernées et informer ces personnes de la portée de leur accord, ou alors faire valoir un intérêt prépondérant à cette modification.

Toute personne qui dispose d'un fichier doit s'assurer que les données contenues dans le fichier sont **correctes**. En d'autres termes, il faut d'une part que les données soient à jour et d'autre part qu'elles puissent être rectifiées si elles sont inexactes.

Tout traitement de données personnelles constitue une atteinte à la personnalité et il faut donc veiller à limiter le plus possible cette atteinte. Pour cette raison, le maître de fichier n'a le droit de traiter que les données dont il a absolument besoin et qui sont pertinentes pour l'accomplissement de ses tâches (principe de la **proportionnalité**).

La collecte de données personnelles et en particulier le but de leur traitement doivent être reconnaissables pour la personne concernée. L'exigence de reconnaissabilité instaurée par la révision de la LPD concrétise le principe de la bonne foi et vise ainsi à rendre le traitement des données plus transparent. Ce principe signifie que la personne concernée doit pouvoir reconnaître, dans des conditions normales, que des données la concernant ont été collectées ou pourraient l'être (prévisibilité). Cette personne doit notamment connaître le but du traitement des données ou pouvoir constater que le but a été indiqué lors de la collecte ou qu'il ressort des circonstances.

Vous devez donc supprimer les données lorsque vous n'en avez plus besoin. Toute personne qui ne respecte pas ces principes porte atteinte à la personnalité de la personne concernée. Une telle atteinte ne se justifie que lorsque le maître du fichier peut faire valoir un motif justificatif tel que l'accord de la personne concernée, un intérêt public ou privé prépondérant, ou une loi (art. 13 LPD).

2.2 Collecte de données

Conformément aux principes qui viennent d'être évoqués, vous ne pouvez collecter que les données dont vous avez impérativement besoin pour atteindre votre objectif.

Une des conditions nécessaires pour garantir qu'un traitement ou une utilisation de données personnelles soit conforme au droit est une collecte des données faite dans le strict respect du droit (art. 13 LPD). La liste de contrôle figurant ci-dessous vous aidera sur ce point.

Lorsque vous collectez des données, vous devez en informer les personnes au sujet desquelles les données sont recueillies, si cela ne ressort pas clairement des circonstances.

Nous vous conseillons de vérifier l'exactitude des données. Vous vous épargnerez ainsi des demandes de renseignements inutiles.

2.3 Communication de données à des tiers

La communication de données à des tiers n'est autorisée que dans des cas bien définis et à certaines conditions (art. 13 LPD). Veuillez vous assurer que vous respectez les principes régissant le traitement des données.

La communication de données est notamment autorisée lorsqu'un intérêt prépondérant privé ou public ou une loi le prévoit.

2.3.1 Traitement de données par des tiers

En tant qu'entreprise, vous pouvez confier le traitement de données personnelles à un tiers dans la mesure où aucune obligation légale ou contractuelle ne vous impose de garder le secret. Mais en votre qualité de mandant vous devez veiller à ce que les données soient traitées de la même façon que vous seriez autorisé vous-même à le faire. En tant que maître du fichier, vous restez donc responsable du traitement des données.

2.4 Déclaration des fichiers

Les personnes privées doivent déclarer leurs fichiers au PFPDT lorsqu'elles traitent régulièrement des données sensibles ou des profils de la personnalité ou lorsqu'elles communiquent régulièrement des données personnelles à des tiers (art. 11a, al. 3, LPD).

L'obligation de déclarer un fichier tombe si les conditions figurant à l'art. 11a, al. 5, LPD et à l'art. 4 OLPD sont remplies, notamment si le maître du fichier a désigné un conseiller à la protection des données indépendant chargé d'assurer l'application interne des dispositions relatives à la protection des données et de tenir un inventaire des fichiers (art. 11a, al. 5, let. e, LPD).

Vous pouvez déclarer vos fichiers soit en remplissant le formulaire idoine à télécharger sur le site www.leprepose.ch, soit en le faisant en ligne à l'adresse www.datareg.admin.ch.

2.5 Communication de données à l'étranger

La communication à l'étranger de données personnelles dont le traitement ne pose aucun problème en Suisse peut, à terme, s'avérer problématique pour la personne concernée, celle-ci étant susceptible, dans certains cas, de perdre le contrôle des données la concernant. Le risque d'une atteinte à la personnalité est donc accru. Pour cette raison, le maître du fichier est tenu de garantir la protection des données même en cas de communication des données à l'étranger.

Des problèmes peuvent par exemple apparaître lorsqu'une association de soutien aux personnes malades du sida communique la liste de ses membres à une organisation partenaire sise dans un pays qui n'assure pas un niveau de protection des données adéquat. Dans un tel cas de figure, si ces données devaient être communiquées à des tiers, il se pourrait, dans certaines circonstances, que l'une ou l'autre des personnes concernées ait des problèmes le jour où elle souhaite se rendre dans le pays en question.

2.5.1 Conditions à remplir

Il est souvent difficile pour les personnes traitant des données d'évaluer les risques d'un transfert. On considère donc que la personnalité des personnes concernées est gravement menacée lorsque le pays dans lequel les données sont transférées n'assure pas un niveau de protection des données adéquat (art. 6, al. 1, LPD).

En principe, on peut partir de l'idée que les Etats qui ont ratifié la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et qui ont signé le protocole additionnel correspondant assurent un niveau de protection adéquat. Tel est notamment le cas pour les pays de l'UE.

Pour faciliter l'évaluation de la situation en cas de communication de données à l'étranger (et à titre d'information pour les personnes concernées), le PFPDT a établi une liste des Etats ayant une législation assurant un niveau de protection des données adéquat. Cette liste peut être consultée à l'adresse www.leprepose.ch.

Le transfert de données personnelles vers des pays qui n'assurent pas un niveau de protection des données adéquat ne doit intervenir que si les conditions prévues à l'art. 6, al. 2, LPD sont remplies.

2.5.2 Contrat

Un système équivalent de protection des données ne garantit cependant pas à lui seul que toute atteinte à la personnalité pourra être évitée. Il est donc conseillé dans tous les cas d'établir un contrat entre le maître du fichier et le destinataire des données, contrat qui réglera la protection et la sécurité des données.

Lorsqu'un fichier est transféré vers un Etat qui ne possède pas de système de protection des données équivalent, il est obligatoire de conclure un tel contrat. De plus, le transfert doit être déclaré au Préposé fédéral à la protection des données et à la transparence (voir chapitre suivant).

2.5.3 Déclaration

La communication de données à l'étranger visée à l'art. 6, al. 2, let. a et g, LPD doit être annoncée au PFPDT (art. 6, al. 3, LPD).

2.6 Obligation de fournir des renseignements

Toute personne dont vous traitez les données dans un fichier a le droit de demander gratuitement des renseignements sur les données en question pour exiger, le cas échéant, qu'elles soient rectifiées ou supprimées.

Vous devez fournir les renseignements demandés dans les 30 jours. Si vous restreignez le droit d'accès, vous avez également 30 jours pour en informer la personne concernée, sous la forme d'une décision écrite motivée. Il ne peut y avoir restriction que lorsqu'une loi au sens formel le prévoit ou que les intérêts prépondérants du maître de fichier ou d'un tiers le justifient et que les données ne sont pas communiquées à des tiers (art. 9 LPD).

La personne concernée peut faire valoir son droit d'accès auprès du juge civil qui statue selon une procédure simple et rapide.

2.6.1 Gratuité des renseignements et exceptions

Les renseignements sont en règle générale fournis gratuitement, car la demande de renseignements est un droit fondamental qui garantit la protection de la personnalité; l'exercice de ce droit ne peut donc être soumis à la perception d'un émolument (art. 8, al. 5, LPD).

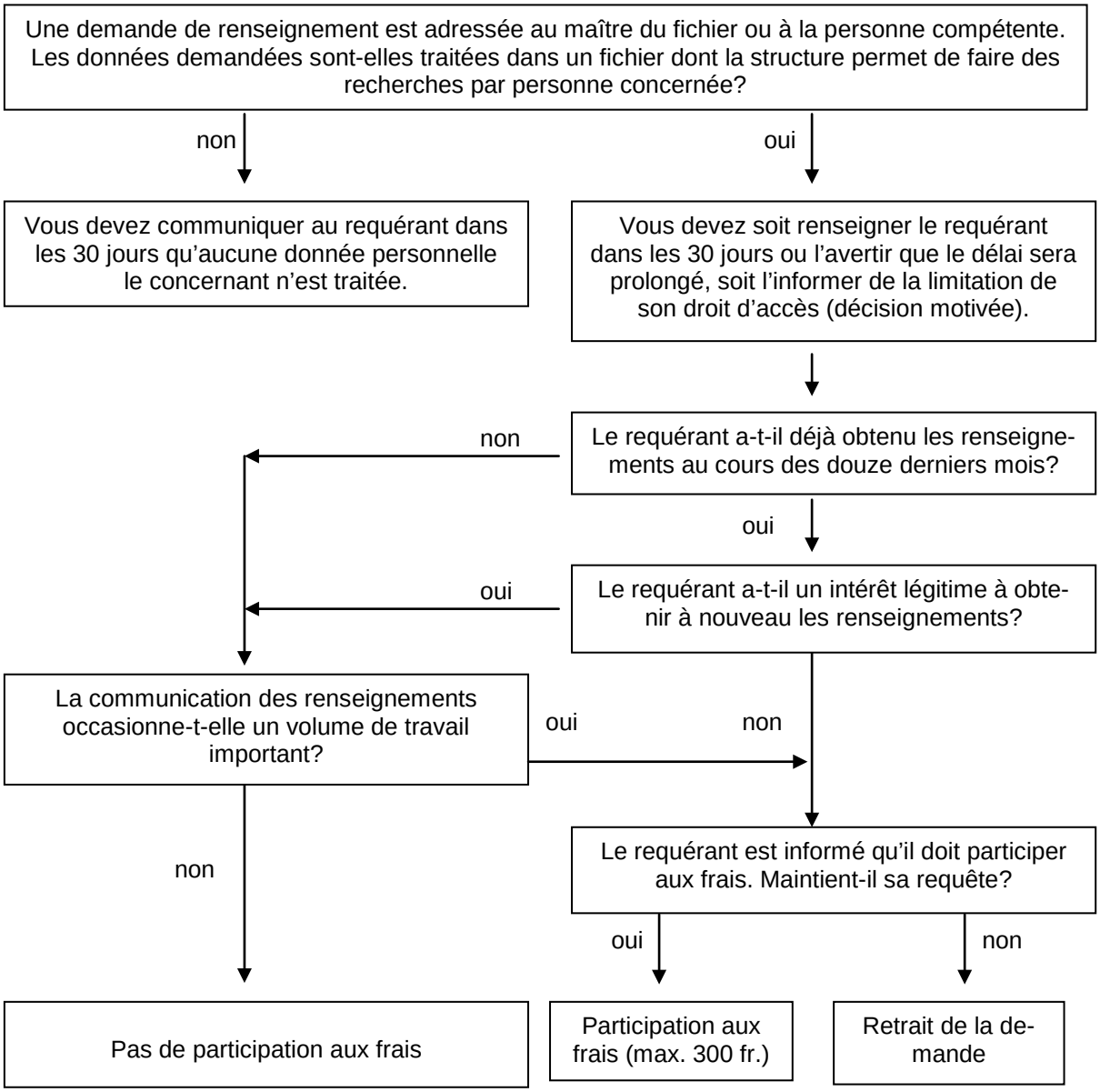
l existe toutefois deux exceptions à cette règle:

- une participation aux frais peut être demandée lorsque les renseignements désirés ont déjà été communiqués au requérant dans les douze mois précédant la demande; le maître du fichier ne peut toutefois pas demander de participation aux frais si le requérant peut se prévaloir d'un intérêt légitime (p. ex. si les données ont changé dans l'intervalle); le but de cette disposition est de limiter le nombre de demandes de renseignements chicanières;

- un émolument peut également être perçu lorsque la communication des renseignements demandés occasionne un volume de travail important (p. ex. parce que les données ont déjà été rendues anonymes) ou qu'il est nécessaire d'effectuer de longues recherches (dans des fichiers manuels); vous ne pouvez cependant pas invoquer une charge de travail importante si l'importance de cette charge est due à une mauvaise organisation ou une mauvaise gestion de votre fichier.

La participation aux frais ne peut être supérieure à 300 francs. Le requérant doit être préalablement informé du montant qu'il devra verser, afin qu'il puisse éventuellement retirer sa requête.

Tableau récapitulatif:



2.7 Sécurité des données

Alors que la protection des données a pour but de protéger la personnalité, la sécurité des données vise à protéger l'information, autrement dit à garantir sa confidentialité, sa disponibilité et son intégrité. La sécurité des données comprend toutes les mesures qui doivent être prises par les maîtres de fichier pour satisfaire aux exigences posées par la loi sur la protection des données.

L’art. 7 LPD prévoit que les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. Ces mesures comprennent entre autres le contrôle de l’accès aux données, le transport, la communication, la mémorisation, l’utilisation et l’entrée des données. Le maître du fichier est tenu de journaliser les traitements de données effectués et d’établir un règlement régissant le traitement.

Le détail des mesures prescrites peut être consulté aux art. 8 à 12 OLPD.

2.8 Dispositions pénales

Le maître d’un fichier est punissable s’il ne respecte pas l’une des trois obligations suivantes: obligation de fournir des renseignements aux personnes concernées, obligation de déclarer les fichiers et les transferts de fichiers à l’étranger, obligation de collaborer avec le Préposé fédéral à la protection des données et à la transparence lors de l’établissement des faits (art. 34 LPD).

Gardez donc à l’esprit que les règles de la protection des données doivent être respectées à chaque fois qu’un particulier mémorise et/ou traite des données dans un fichier dont la structure permet de faire des recherches par personne concernée.

3. Quelques indications utiles pour «démarrer» dans la protection des données

Si vous traitez des données, commencez par établir une liste de tous vos fichiers dont la structure permet de rechercher des données par personne. Cette mesure vous permettra de déterminer qui collecte des données, quelles données sont collectées et dans quel but. Cette liste vous aidera à mettre en œuvre de façon plus efficace les mesures nécessaires à un traitement correct des données.

Nous vous recommandons de désigner un organe interne qui veillera à ce que les règles de protection des données soient respectées. Les expériences faites en Allemagne ces trente dernières années dans le domaine de la protection des données ont montré qu'il était absolument indispensable, dans les grandes entreprises du moins, de désigner un organe responsable.

Nous vous conseillons également d'informer vos collaborateurs des dispositions prévues dans la LPD concernant le traitement des données personnelles. Faites par exemple circuler une note présentant les dispositions de la loi, et attirez l'attention de vos collaborateurs sur les principes régissant le traitement des données personnelles (but du traitement, transmission de données personnelles, etc.). De plus, vous pouvez, par écrit, soumettre vos employés à l'obligation de respecter le secret professionnel (art. 35 LPD).

Il est indispensable de prévoir une planification et une coordination dans le domaine de la protection des données. Dans le cas contraire, vous ne pourrez que difficilement satisfaire à toutes les exigences qui sont posées dans ce domaine si complexe.

Pensez-y: un traitement de données qui ne respecte pas les principes de la protection des données peut nuire à votre image ainsi qu'à celle de votre entreprise.

4. Annexe: Définitions selon la loi fédérale sur la protection des données

Données personnelles:	Toutes les informations qui se rapportent à une personne identifiée ou identifiable.
Personne concernée:	La personne physique ou morale (personne physique, entreprises, association) au sujet de laquelle des données sont traitées.
Données sensibles:	Les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, des mesures d'aide sociale, des poursuites ou sanctions pénales ou administratives.
Profil de la personnalité:	Un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique.
Traitement:	Toute opération relative à des données personnelles - quels que soient les moyens et procédés utilisés - notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données.
Communication:	Le fait de rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant.
Fichier:	Tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée.
Organe fédéral:	L'autorité ou le service fédéral ainsi que la personne en tant qu'elle est chargée d'une tâche de la Confédération (par ex. les caisses maladies).
Maître du fichier:	La personne privée ou l'organe fédéral qui décide du but et du contenu du fichier.