Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Office fédéral de la justice OFJ
Domaine de direction Droit public
Unité Projets et méthode législatifs

Loi sur la protection des données, modification du 24 mars 2006 : questions fréquentes concernant le traitement de données par des personnes privées

1. Questions générales

11	Les modes de traitement et les fichiers existant avant l'entrée en vigueur de la modification doivent-ils être adaptés ?

Les nouvelles dispositions ne distinguent pas entre fichiers ou traitements anciens et nouveaux. Dans la mesure où les fichiers existants continuent d'être réellement utilisés et que des données continuent d'être traitées, il faut adapter les processus au nouveau droit. On tiendra principalement compte des points suivants :

- Reconnaissabilité, devoir d'information : un délai d'un an est prévu pour prendre les mesures nécessaires afin d'assurer la reconnaissabilité de la collecte et l'information des personnes concernées (cf. ch. 2).

- Communication transfrontière de données : lorsque des données personnelles sont communiquées à l'étranger et que l'Etat en question ne possède pas une législation qui assure un niveau de protection adéquat, il faut examiner si le destinataire des données peut fournir des garanties, par exemple sous forme d'une clause contractuelle (cf. ch. 4). Ces garanties ne sont pas nécessaires si une des exceptions mentionnées à l'art. 6, al. 2, LPD s'applique (notamment si la personne concernée a donné son consentement, ou si la communication a lieu au sein d'un même groupe de sociétés appliquant des règles de protection des données appropriées).

- Obligation de déclarer les fichiers : il faudra à l'avenir déclarer certains fichiers qui ne devaient pas l'être auparavant (cf. ch. 7). Le Préposé fédéral à la protection des données et à la transparence (PFPDT) appliquera dans ces cas-là par analogie l'art. 38 LPD (Dispositions transitoires) ; en d'autres termes, il y aura un délai d'un an pour déclarer ces fichiers.

Référence : nouveaux art. 4, al. 4, et 7a LPD, FF 2003 1958 (reconnaissabilité, devoir d'information) ; nouvel art. 6 LPD, nouvel art. 5 OLPD, FF 2003 1940 ss (communication transfrontière de données) ; nouvel art. 11a LPD, nouveaux art. 1 à 4 OLPD, FF 2003 1948 s. (obligation de déclarer les fichiers).

12	En cas de doute dans l'interprétation des nouvelles dispositions de la LPD, peut-on s'appuyer sur l'interprétation de la directive européenne 95/46/CE sur le traitement des données par une autorité étrangère de protection des données ?

La révision rapproche le droit suisse de la directive européenne sur plusieurs points. L'interprétation de la directive par les autorités étrangères de protection des données ou par le groupe visé à l'art. 29 de ce texte peut, sur ces points, donner des indications quant à leur application pratique. S'il s'agit de concrétiser un des principes matériels en matière de protection des données, on peut en général considérer qu'une pratique conforme à la directive satisfera aux exigences de la LPD.

2 Transparence

21 Caractère reconnaissable de la collecte et des finalités du traitement (art. 4, al. 4)

211	A quelles conditions peut-on dire que la collecte et les finalités du traitement sont reconnaissables ?

Le nouvel art. 4, al. 4, ne change fondamentalement rien. On déduisait déjà du principe de la bonne foi (art. 4, al. 2) que la collecte de données, les finalités de leur traitement et l'identité de la personne qui les traite doivent être reconnaissables. Dans de nombreux cas, notamment dans les transactions courantes, aucune mesure particulière n'est nécessaire. Ce qui est déterminant, c'est que le destinataire ou le client moyen (fictif) soit en mesure de reconnaître dans des circonstances concrètes que des données sont collectées à son sujet, par qui, à quelle fin, et à qui elles seront éventuellement communiquées.

Référence : nouvel art. 4, al. 4, LPD ; FF 2003 1937 ss.

212	A quel moment doivent-elles être reconnaissables ?

Normalement, la collecte doit être reconnaissable au moment même où elle a lieu. Il faut au moins que le moment précis où les données ont été collectées soit connu.

Cependant, si le fait que la collecte de données soit reconnaissable sur le moment même compromettait la finalité du traitement ou que l'on ne puisse exiger de celui qui traite les données qu'il indique l'instant précis de la collecte (notamment si cela occasionne un travail excessif), deux façons de procéder sont possibles en pratique, selon les circonstances : mentionner, par une indication générale ou dans une clause contractuelle, que des données seront collectées ultérieurement, ou rendre la collecte reconnaissable après coup.

Plus les données personnelles sont sensibles, plus la personne qui les traite est tenue de rendre la collecte reconnaissable sur l'instant, ou bien plus elle doit faire valoir un intérêt important pour ne pas le faire.

Les principes applicables sont les mêmes lorsque, au moment d'une transaction (p. ex. la conclusion d'un contrat), il n'est pas encore clair si des données supplémentaires seront collectées (ou s'il existe simplement une possibilité que de telles données soient collectées) : en règle générale, les personnes concernées doivent être informées au moment concret de la collecte de données. Une simple indication de l'éventualité d'une collecte de données ultérieure ne suffit pas si des données sensibles ou des profils de la personnalité sont collectés et traités.

Les principes exposés ici s'appliquent également aux explications relatives à l'art. 7a (cf. ch. 222).

213	Peut-on considérer de manière générale qu'une communication de données est reconnaissable si elle a lieu au sein d'un groupe de sociétés ?

Non. Il n'est pas possible de présumer tout simplement qu'une communication est reconnaissable pour la personne concernée, même si le destinataire des données appartient à la même personne juridique. Si deux sociétés du même groupe travaillent dans des domaines différents ou qu'elles sont connues à l'extérieur sous des désignations différentes, il faut prendre des mesures appropriées pour garantir la reconnaissabilité.

214	A quelles conditions peut-on collecter et traiter des données sans assurer la reconnaissabilité ?

Il est possible de collecter et de traiter des données sans que la personne concernée le sache si l'on peut faire valoir un intérêt prépondérant particulier et que la simple reconnaissabilité soit de nature à compromettre les finalités du traitement. Lorsque c'est faisable, il convient d'indiquer au préalable, de manière générale, que des données peuvent être collectées à l'insu des personnes concernées, dans certaines circonstances – ces circonstances devant être décrites aussi précisément que possible. L'information peut par exemple avoir lieu lors de la conclusion du contrat (s'il y a relation contractuelle) ou s'inscrire dans des directives aux collaborateurs (s'il s'agit p. ex. de lutter contre l'utilisation abusive des infrastructures de communication de l'employeur).

Une disposition légale peut aussi prévoir que des données peuvent être collectées sans que cela soit reconnaissable pour la personne concernée.

215	Comment faut-il procéder (p. ex. en cas de reprise de société) pour intégrer une banque de données étrangère dans son propre fichier ?

Si le maître du fichier change, c'est un des éléments essentiels du traitement de données qui change. La personne à laquelle se rapportent les données doit être consciente de cette modification. Selon la nature des données traitées et la finalité du traitement, diverses mesures sont nécessaires, même si la finalité du traitement ne change pas et que les données ont été traitées légalement jusque-là :

- Pour le simple traitement de données qui sont de toute façon publiques ou qui sont peu sensibles pour d'autres raisons (p. ex. le traitement d'adresses à des fins publicitaires), le traitement est reconnaissable dès lors qu'il y a une communication avec la personne concernée (p. ex. un envoi personnel de publicité).

- S'il s'agit de données plus délicates qui peuvent toucher les intérêts essentiels des personnes concernées (p. ex. des données sur le client d'une banque), il convient d'annoncer à l'avance le changement de maître du fichier en donnant à la personne concernée la possibilité de refuser la transmission des données.

- S'il s'agit de données sensibles ou de profils de la personnalité, l'art. 7a s'applique : la personne concernée doit être informée (cf. ch. 3 ci-dessous), avec mention expresse du fait qu'elle peut refuser la transmission des données.

Référence : nouveaux art. 4, al. 4, et 7a LPD ; FF 2003 1937 ss, 1943 ss, 5e rapport d'activités PFPDT, 168.

216	Comment faut-il procéder pour la collecte de données auprès de tiers ?

La collecte de données auprès d'une tierce personne doit également être reconnaissable pour la personne concernée. Là aussi, la reconnaissabilité peut être assurée à l'avance, par une information inscrite dans un contrat ou dans des conditions générales.

217	Faut-il aussi assurer la reconnaissabilité lorsque les données sont collectées à partir de sources accessibles à tous (p. ex. sur Internet) ?

En ce cas, il n'est en principe pas nécessaire de prendre des mesures particulières. Il y a obligation d'informer si les données recueillies servent à composer un profil de la personnalité (cf. ch. 22 ci-dessous). En outre, lorsque la personne concernée a expressément refusé

que des données soient traitées à certaines fins, il est interdit d'aller à l'encontre de sa volonté.

22 Devoir d'informer lors de la collecte de données sensibles et de profils de la personnalité (art. 7a)

221 Quelles informations faut-il donner à la personne concernée ?

Le nouvel art. 7a, al. 2, décrit les informations minimales à donner : identité du maître du fichier, finalités du traitement et catégories de destinataires de données. Suivant le contexte, il faudra aussi indiquer à la personne concernée si elle est tenue de fournir des données la concernant et quelles sont les conséquences d'un refus.

Il n'est pas nécessaire d'indiquer l'identité de chaque destinataire des données.

Référence : nouvel art. 7a, al. 2, LPD ; FF 2003 1943 ss.

222 Quand et comment faut-il donner ces informations ?

Les informations doivent être données en principe au moment de la collecte. Pour plus de renseignements sur le moment de l'information, voir plus haut ch. 212.

Les informations doivent être données expressément, mais aucune forme déterminée n'est prescrite. S'il est souvent utile de procéder par écrit, il est aussi possible d'informer la personne concernée par oral (p. ex. en cas de sondage par téléphone ou de consultation par téléphone d'un centre de conseil médical).

Référence : nouvel art. 7a LPD ; FF 2003 1943 ss.

223 A quelles conditions peut-on collecter et traiter des données sensibles sans que la personne concernée doive en être informée ?

Il est possible de ne pas informer la personne concernée – ou de l'informer après coup – si une loi au sens formel le prévoit, si des intérêts prépondérants de tiers le requièrent ou si des intérêts prépondérants du maître du fichier le requièrent et qu'il ne communique pas les données à des tiers (voir plus haut ch. 212, 214 et 222).

Référence : nouveaux art. 7a et 9 LPD, FF 2003 1943 ss.

224 Quand faut-il informer la personne concernée si l'on collecte des données susceptibles de constituer, avec le temps, un profil de la personnalité ?

La personne concernée doit être informée aussi tôt que possible. Dès qu'il ressort des finalités du traitement qu'un profil de la personnalité pourrait se dessiner, les personnes concernées doivent être informées.

225 Faut-il informer la personne concernée conformément à la nouvelle disposition si l'on traitait déjà des données sensibles avant l'entrée en vigueur de la modification (ou si le fichier existait déjà à cette date) ?

Non. Le devoir d'information ne s'applique pas rétroactivement aux données déjà collectées. Par contre, selon le nouvel art. 7a, il faut informer les personnes concernées si l'on collecte

de nouvelles données dans le cadre du traitement en cours (dans la mesure où elles n'ont pas été suffisamment informées auparavant) ou si l'on collecte des données relatives à de nouvelles personnes.

Référence : FF 2003 1958.

3. Définition du consentement (art. 4, al. 5)

31	Le consentement de la personne concernée est-il nécessaire pour tout traitement de données personnelles ?

Non. L'art. 4, al. 5, donne simplement une définition de ce terme en décrivant les critères auxquels le consentement doit satisfaire lorsque la loi en fait une condition du traitement de données (art. 6, al. 2, let. b [nouvelle], 13, al. 1, 17, al. 2, let. c, 19, al. 1, let. b, LPD).

32	Que veut dire « dûment informée » dans la perspective d'un consentement ?

Les personnes à propos desquelles des données sont traitées doivent être informées d'une part des éléments essentiels du traitement (cf. plus haut ch. 211 et 221), d'autre part des conséquences d'un refus du consentement, notamment des inconvénients que cela pourrait entraîner pour elles. Elles doivent disposer de toutes les informations nécessaires pour exprimer leur volonté en pleine connaissance de cause.

L'information peut être donnée par écrit (sur papier, à l'écran, par SMS), par téléphone ou oralement. Il n'existe aucune exigence de forme.

33	Que veut dire « exprimer sa volonté librement » ?

La personne concernée ne donne pas son consentement librement si les désavantages qu'aurait entraîné pour elle un refus - et dont elle doit avoir été informée - sont sans rapport avec les finalités du traitement ou qu'ils sont disproportionnés par rapport à ces dernières.

Référence : FF 2003 1939 s.

34	Sous quelle forme le consentement doit-il être donné ?

Le consentement ne doit pas revêtir de forme particulière. Il peut être tacite ou ressortir d'actes concluants. Mais en cas de traitement de données sensibles ou de profils de la personnalité, le consentement doit être exprès. La forme écrite est recommandée à titre de preuve. Il est en principe possible de donner son consentement par la voie électronique, par exemple d'un clic de souris sur un formulaire Internet, qu'il s'agisse ou non de données sensibles et de profils de la personnalité (mais il faut que les conditions et les processus soient aménagés de telle sorte que l'authentification de la personne concernée et la sécurité de la transmission soient assurées de manière adéquate).

Référence : FF 2003 1939 s.

4. Communication transfrontière de données (art. 6)

41	Quelles sont les conséquences de la modification des notions utilisées ?

La teneur de l'art. 6, al. 2, LPD est modifiée en ce sens que l'ancienne disposition se référait à la transmission de fichiers. Désormais, la référence est faite de façon plus générale à la communication de « données personnelles ». Dans la pratique, cette nuance n'implique pas de modification importante, car tout ensemble d'informations contenant des données relatives à plus d'une personne constitue en principe un fichier selon l'interprétation actuelle.

D'autre part, selon l'ancienne disposition, la personne concernée était gravement menacée notamment du fait de l'absence, dans l'Etat destinataire, d'une « protection des données » équivalente à celle qui est garantie en Suisse. La nouvelle disposition se réfère, quant à elle, à l'absence d'une « législation » assurant un niveau de protection adéquate, ce qui constitue le critère déterminant. En effet, si ce critère n'est pas rempli, des données personnelles ne peuvent être communiquées à l'étranger qu'à l'une des conditions énumérées au nouvel art. 6, al. 2, LPD. La personne qui traite les données est d'autant plus tenue, dans de tels cas, de veiller à ce que la protection des données personnelles soit suffisamment assurée.

Références : nouvel art. 6 LPD ; FF 2003 1940 ss.

42	Est-il toujours possible de déroger à l'art. 6 lorsque la personne qui traite les données peut faire valoir des intérêts prépondérants ?

Jusqu'à présent, la personne qui traite les données pouvait, sur la base d'un motif justificatif figurant sur la liste non exhaustive de l'art 13 LPD, à savoir n'importe quel intérêt privé prépondérant, déroger à l'interdiction de principe de communiquer des données vers un Etat destinataire ne disposant pas d'une protection des données équivalente à celle de la Suisse. En revanche, le nouvel art. 6, al. 2, énumère de manière exhaustive les conditions nécessaires à une communication licite vers un Etat ne disposant pas d'une législation assurant un niveau de protection adéquat. En l'absence d'une telle législation dans l'Etat destinataire, la personne qui traite les données doit, dans tous les cas, veiller à ce que des garanties suffisantes permettent d'assurer la protection des données, pour autant qu'une des autres conditions ne soit pas remplie.

43	La publication de données personnelles sur Internet est-elle assimilée à une communication à l'étranger ?

La publication de données personnelles sur Internet ou au moyen d'autres services d'information et de communication automatisés n'est pas assimilée à une communication à l'étranger. Lorsque des données personnelles sont publiées sur Internet à des fins d'information du public, notamment par le biais des médias, le fait que ces informations puissent aussi être consultées à l'étranger n'est qu'une conséquence de leur publication sur Internet. Les autres exigences juridiques résultant notamment de la législation relative à la protection des données et de la personnalité doivent évidemment être respectées.

Référence : nouvel art. 5 OLPD

44	Que signifie « en l'espèce » en relation avec un consentement ou une communication ?

Ce terme est à interpréter de telle sorte que plusieurs communications relatives à des données personnelles d'une même personne et effectuées aux mêmes conditions (destinataire, finalité, transmission éventuelle) doivent être considérées comme un seul cas d'espèce ; par exemple, la personne n'aura à donner son consentement qu'une seule fois. En outre, cette

formulation indique que chaque communication doit concerner un cas concret, par exemple en relation avec la constatation d'un droit en justice.

Référence : FF 2003 1940 ss.

45 Quand une communication est-elle en « relation directe » avec la conclusion ou l'exécution d'un contrat ?

Les traitements de données sont en relation directe avec la conclusion ou l'exécution d'un contrat au premier chef lorsqu'ils se réfèrent à la conclusion d'un contrat prévue par les parties concernées (p. ex. un appel d'offres). On entend par exécution d'un contrat l'accomplissement des obligations principales et secondaires inscrites dans ledit contrat. La communication est autorisée dès lors que les prestations découlant du contrat incluent ou exigent une telle communication. Il peut s'agir par exemple de la communication de données personnelles concernant le cocontractant à des sociétés de renseignements sur les crédits à des fins de vérification de la solvabilité, de la transmission de données par une agence de transport dans le cadre de la livraison de biens, de mandats dans le trafic international des paiements, de prestations de transport internationales (voyages en train, en bateau ou en avion), de la réservation d'hôtels ou de voitures de location.

46 Quand le maître du fichier doit-il partir du principe que la personne concernée s'oppose au traitement de données rendues accessibles à tout un chacun ?

La personne qui souhaite que des données qu'elle a elle-même rendues publiques ne soient pas traitées à certaines fins ou soient traitées à des fins précises doit le mentionner explicitement. Par ailleurs, elle pourrait communiquer à une personne traitant des données qu'elle ne souhaite pas que les données publiées la concernant soient traitées (cf. l'art. 12, al. 2, let. b, LPD).

47 A quelles exigences les règles de protection des données appliquées au sein d'un groupe de sociétés doivent-elles répondre pour pouvoir compenser l'absence d'une législation adéquate en la matière ?

Pour que les règles de protection des données appliquées au sein d'un groupe de sociétés puissent compenser l'absence de législation adéquate en matière de protection des données dans l'Etat destinataire, il faut qu'elles répondent aux exigences suivantes:

- sur le plan matériel, elles doivent répondre au minimum aux exigences de la Convention STE n° 108 du Conseil de l'Europe et du protocole additionnel posées aux personnes privées ;

- le caractère obligatoire des règles imposées à chacune des sociétés du groupe doit être assuré sur le plan formel et dans la pratique ;

- le PFPDT doit être informé des règles appliquées.

Sur le plan formel, le caractère obligatoire peut, par exemple, être assuré par une décision du conseil d'administration, que les différentes sociétés seront tenues de reprendre et d'appliquer. Dans la pratique, la mise en œuvre peut être assurée par exemple par des audits internes.

Il n'est pas nécessaire que les règles soient approuvées par les autorités compétentes en matière de protection des données dans l'Etat destinataire (ou dans les Etats destinataires).

48	Comment le PFPDT doit-il être informé des garanties et des règles de protection des données appliquées dans un groupe de sociétés ?

Le PFPDT ne doit pas être informé de chaque communication de données. Il peut l'être de manière globale lorsque les données sont communiquées dans un domaine précis de manière régulière, conformément à des contrats ou des clauses contractuelles standards biens déterminés.

Tant que les règles de protection des données annoncées assurent un niveau de protection adéquat, il n'y a pas lieu de communiquer au PFPDT chaque modification apportée.

Si la personne qui traite les données a recours de manière générale aux contrats et clauses contractuelles standards reconnus par le PFPDT, il n'y a lieu d'en informer qu'une seule fois le PFPDT. Celui-ci publiera une liste des contrats et des clauses reconnus. Sont reconnus dans tous les cas les modèles de l'UE, du Conseil de l'Europe et ceux que le PFPDT a lui-même établis (cf. le site Internet du PFPDT: http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=fr).

L'information peut être transmise par voie électronique. Le PFPDT indiquera quelles sont les modalités requises en temps utile.

Le PFPDT examine les garanties et les règles de protection des données qui lui sont annoncées et communique le résultat de son examen au maître du fichier dans un délai de 30 jours à compter de la date de leur réception. S'il n'a pas réagi ni formulé de réserves dans le délai fixé, le maître du fichier peut partir de l'idée que les garanties ou les règles de protection des données appliquées dans le groupe de sociétés répondent aux exigences.

Référence : nouvel art. 6 LPD; nouvel art. 6 OLPD; FF 2003 1940 ss.

49	La liste des Etats disposant d'une législation assurant un niveau de protection adéquat qui doit être établie par le PFPDT est-elle contraignante et exhaustive ?

Si la personne qui traite les données en communique à destination d'un Etat mentionné dans la liste, il peut invoquer sa bonne foi. En revanche, s'il a pu constater sur la base de son expérience que les prescriptions en matière de protection des données ne sont, d'une manière générale ou dans certains domaines, pas respectées dans cet Etat, il ne peut plus faire valoir sa bonne foi.

La liste n'a pas une valeur exhaustive, car il est possible que certains Etats ne disposent d'une législation adéquate que dans certains domaines spécifiques.

Référence : nouvel art. 7 OLPD

5. Droit d'accès (art. 8, al. 2)

51	Sera-t-il obligatoire à l'avenir d'indiquer l'origine des données dans le fichier ?

Non. En vertu de la nouvelle teneur de l'art. 8, al. 2, let. a, LPD, le droit d'accès se limite aux informations « disponibles » sur l'origine des données. La personne qui traite les données est libre de saisir ces informations. Cependant, les effacer à la réception d'une demande d'accès, dans le seul but de ne pas devoir fournir de renseignement, reviendrait à faire preuve de mauvaise foi.

Référence : nouvel art. 8, al. 2, LPD; FF 2003 1946 s.

52	La « protection des sources » sera-t-elle encore possible à l'avenir ?

Si la communication des renseignements demandés sur l'origine des données porte atteinte aux intérêts prépondérants de tiers, elle peut être restreinte conformément à l'art. 9 LPD. Il en va de même si la communication des renseignements porte atteinte aux intérêts prépondérants de le personne qui traite les données, à condition que les données personnelles ne soient pas communiquées à des tiers.

On peut parler d'intérêts prépondérants de tiers lorsque, par exemple, des éléments indiquent que la personne concernée pourrait se montrer violente envers un informateur ou lorsqu'elle est le chef de l'informateur et que ce dernier se trouve, de ce fait, en situation de dépendance. Si le risque encouru consiste uniquement à ce que des tiers puissent subir des désagréments, il convient de conclure à l'absence d'intérêts prépondérants.

53	A l'avenir, les personnes concernées pourront-elles, de manière générale, demander que les renseignements leur soient communiqués par voie électronique ?

La demande d'accès ne doit être adressée par voie électronique que si la personne qui traite les données le prévoit expressément, par exemple lorsqu'il indique sur son site Internet ou dans ses conditions générales que les demandes d'accès peuvent être adressées par courrier électronique à un service spécifique ou au moyen d'un formulaire électronique et que des moyens de sécurité et d'identification sont mis en place.

Référence : nouvel art. 1, al. 2, OLPD

6. Traitement de données par un tiers (art. 10a)

	Quelles sont les obligations du mandant à l'égard du mandataire ?

Concernant le traitement de données par un tiers (externalisation), les exigences ne sont pas fondamentalement modifiées par rapport à l'ancien droit. La nouvelle disposition prévoit toutefois que le traitement de données par un tiers n'est possible que si une convention ou une loi le prévoit. Pour les personnes privées, cela signifie que l'attribution d'un mandat doit faire l'objet d'un contrat.

La loi précise par ailleurs l'obligation du mandant de s'assurer que le mandataire applique les mêmes normes de protection et de sécurité des données que celles qu'il serait lui-même tenu d'appliquer. Il doit en outre s'assurer que les mesures nécessaires sont réellement prises, par exemple en se rendant sur place pour le vérifier. En revanche, le mandant n'est pas tenu de surveiller en permanence le traitement des données par le mandataire. Si ce dernier dispose d'une certification selon l'ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données, le mandant peut considérer que les données sont traitées de manière conforme aux exigences légales.

Référence : nouvel art. 10a LPD ; FF 2003 1947

7. Obligation de déclarer les fichiers (art. 11a)

71	Faut-il désormais déclarer des fichiers qui n'étaient précédemment pas soumis à l'obligation de déclarer ?

Par rapport à l'ancien droit, la loi révisée étend la portée de l'obligation de déclarer les fichiers. Les fichiers devront ainsi être déclarés même lorsque les personnes sont informées du traitement de données les concernant. En contrepartie, des exceptions générales sont prévues lorsque la personne qui traite les données engage un conseiller à la protection des

données indépendant et l'annonce au PFPDT, ou qu'elle obtient une certification. Par ailleurs, les exceptions prévues dans l'ordonnance ont été adaptées ; ne sont désormais plus soumis à l'obligation de déclarer, par exemple, les fichiers de fournisseurs et de clients, pour autant qu'ils ne contiennent pas de données sensibles.

Les fichiers qui n'étaient jusqu'à présent pas soumis à l'obligation de déclarer devront donc être déclarés au PFPDT lorsqu'ils ne répondent à aucun des motifs d'exception nouvellement prévus. Pour la déclaration de ces fichiers, le PFPDT appliquera par analogie l'art. 38 LPD et accordera donc pour la déclaration un délai d'un an à compter de l'entrée en vigueur de la modification.

Référence : nouvel art. 11a LPD ; FF 2003 1948 s.

72 Qui doit déclarer le fichier lorsque les données sont traitées par un tiers (externalisation) ?

C'est le maître du fichier qui doit faire la déclaration. En l'absence d'un des motifs d'exceptions prévus (cf. plus haut ch. 71), il est tenu de déclarer le fichier même s'il ne traite pas les données lui-même.

73 Les systèmes de courrier électronique, les fichiers journaux (logfiles) et les fichiers de sauvegarde (backups) doivent-ils être déclarés ?

Les données accumulées dans des systèmes de communication électronique (p. ex. messagerie électronique) ne sont en principe pas considérées comme des fichiers autonomes. En règle générale, un système de communication électronique n'est qu'un outil de transmission et n'est pas utilisé pour administrer, structurer ou traiter des données personnelles. Les fichiers qui se constituent dans ce genre de systèmes ne sont dès lors pas soumis à l'obligation de déclarer.

L'ordonnance excepte de l'obligation de déclarer les fichiers journaux et les fichiers archivés qui ne sont plus utilisés activement.

Les fichiers de sauvegarde ne sont pas considérés comme des fichiers autonomes ; il n'est dès lors pas nécessaire de les déclarer en sus.

74 Faut-il déclarer un fichier qu'un collaborateur utilise à titre personnel comme moyen auxiliaire pour son travail ?

Il n'est pas nécessaire de déclarer les fichiers de données personnelles utilisés comme moyens auxiliaires pour l'exécution des tâches dans le cadre du travail. La déclaration n'est en particulier pas nécessaire lorsqu'il s'agit de copies de données provenant d'un fichier qui, lui, est soumis à l'obligation de déclarer.

Sont considérés comme un moyen auxiliaire personnel les documents ou les informations enregistrées sous forme électronique qui ne sont utilisés que par leur auteur ou par un cercle restreint de personnes (p. ex. le suppléant et le supérieur de l'auteur). Exemples :

- copies de travail de lettres enregistrées dans un dossier d'un client ou d'un patient ;
- notes personnelles servant d'aide-mémoire sur les clients qu'un collaborateur enregistre sur son ordinateur ou sur un sous-répertoire personnel du serveur.

75	Les fichiers peuvent-ils être déclarés via Internet ?

Pour les personnes privées, une déclaration via Internet ne sera pas encore possible au moment de l'entrée en vigueur du nouveau droit. Le PFPDT met tout en œuvre pour offrir cette possibilité dans les meilleurs délais.

8. Justification du traitement (art. 12, al. 2)

81	Dans la pratique, quelles conséquences les modifications apportées au mécanisme de justification du traitement des données ont-elles (art. 12, al. 2, LPD) ?

En révisant l'art. 12, al. 2, LPD, le législateur n'entendait pas s'écarter, sur le principe, du système actuel. Son objectif n'était pas d'exclure tout motif justificatif permettant de déroger aux principes généraux de la protection des données, mais :

- de mettre en évidence, par cette reformulation, que les dérogations ne doivent pas être hâtivement justifiées ;

- d'éviter tout malentendu concernant les principes auxquels il n'est pas envisageable de contrevenir (en particulier la bonne foi et la légalité du traitement des données).

Indications relatives à la légalité du traitement des données sous le nouveau droit :

- Présence d'un consentement : le traitement des données est licite s'il est reconnaissable pour la personne concernée (nouvel art. 4, al. 4, LPD) ou que celle-ci a été suffisamment informée (nouvel art. 7a LPD) et si la personne concernée a donné son consentement conformément au nouvel art. 4, al. 5, LPD.

- Intérêts prépondérants de la personne qui traite les données : le principe de proportionnalité contient implicitement l'obligation de prendre en considération les intérêts prépondérants de la personne qui traite les données lors de l'examen de la légalité. Il inclut – y compris dans le cas du traitement de données par des personnes privées – un examen de l'adéquation et de la nécessité et (dans le cadre de l'examen du rapport entre les finalités du traitement et les moyens mis en œuvre) une pesée des intérêts.

- Traitement de données fondé sur une loi spéciale : lorsqu'une loi spéciale prévoit le traitement de données personnelles, celui-ci est en principe licite. L'art. 4, al. 3, LPD actuel, qui fait de la base légale une réserve permettant de déroger au principe de la finalité, l'exprime déjà. On peut citer comme exemples de ces bases légales spéciales les obligations de communiquer des personnes privées prévues par la loi sur le crédit à la consommation[1], la loi sur les épidémies[2] ou la loi sur le blanchiment d'argent[3].

L'OFJ a établi une notice interprétative qui aborde cette question plus en détail. Elle est disponible sur le site Internet de l'OFJ à l'adresse suivante :
http://www.bj.admin.ch/etc/medialib/data/staat_buerger/gesetzgebung/datenschutz.Par.0019.File.tmp/20070111-Auslegungshilfe-d.pdf

[1] Art. 25 ss de la loi fédérale sur le crédit à la consommation, RS 221.214.1
[2] Art. 27 de la loi sur les épidémies, RS 818.101
[3] Art. 9 de la loi sur le blanchiment d'argent, RS 955.0

9. Interdiction du traitement des données (art. 15, al. 1 et 3)

91	Que faut-il entendre par « l'interdiction du traitement des données » ?

La notion d'interdiction du traitement des données provient de la terminologie du droit de l'UE. L'interdiction n'empêche pas de disposer des données, mais impose de renoncer partiellement ou complètement à les traiter. Selon les circonstances, une interdiction peut donc être requise pour toutes les formes de traitement (à l'exception de la conservation des données) ou uniquement pour certains types de traitement (p. ex. la communication à des tiers).

BRU / 30.11.2007 (V. 1.1)