Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Explications sur les modifications du 17 décembre 2004 et du 24 mars 2006 de la loi fédérale sur la protection des données (LPD)

Feldeggweg 1, 3003 Bern
Tel. 031 322 43 95, Fax 031 325 99 96
www.edoeb.admin.ch

Introduction

Le 24 mars 2006, l'Assemblée fédérale a adopté une loi portant révision de la loi fédérale sur la protection des données et adopté l'arrêté fédéral autorisant le Conseil fédéral à ratifier le protocole additionnel du 8 novembre 2001 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. La révision de la LPD (FF 2006 3421 ; FF 2003 1915) poursuit deux objectifs principaux. Il s'agissait tout d'abord de donner suite à la motion 98.3529 de la Commission de gestion du Conseil des Etats « Liaisons on-line : Renforcer la protection pour les données personnelles » et à la motion 00.3000 de la Commission des affaires juridiques du Conseil des Etats « Renforcement de la transparence lors de la collecte des données personnelles ». Il s'agissait ensuite d'adapter la LPD aux exigences du protocole additionnel à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108), en vue de sa ratification.

La loi révisée renforce ainsi la position des personnes concernées en prévoyant une plus grande transparence dans le traitement des données personnelles, avec en particulier l'obligation d'informer les personnes concernées lors de la collecte de données sensibles et de profils de personnalité. Elle revoit le régime des flux transfrontières de données, avec en particulier l'abandon de l'obligation de déclarer les transferts de fichiers à l'étranger. Elle adapte l'annonce des fichiers pour tenir compte des obligations de transparence. Elle innove en introduisant, sous forme de norme incitative, le recours à la certification des produits et des systèmes de traitement des données personnelles et encourage les maîtres de fichier à mettre en place des conseillers à la protection des données. Enfin, le PFPDT pourra également recourir contre les décisions de la Chancellerie fédérale ou départements rejetant une recommandation qu'il aura émise.

Ces modifications entreront en vigueur le 1er janvier 2008.

La LPD a également été partiellement révisée avec l'entrée en vigueur le 1er juillet 2006 de la loi fédérale du 17 décembre 2004 sur le principe de transparence dans l'administration (Loi sur la transparence, LTrans, RS 152.3). Il s'agit en particulier des dispositions sur la communication des données et sur les tâches du préposé fédéral à la protection des données et à la transparence.

Dispositions générales de protection des données

Principes (Article 4)

L'article 4 de la LPD, qui définit les principes de base de la protection des données, a été modifié d'une part pour le rendre plus conforme à l'article 5, let. a de la Convention STE n° 108 et d'autre part pour renforcer la transparence des traitements.

Ainsi à l'alinéa 1, ce n'est pas uniquement la collecte qui doit être licite, mais également toutes les autres phases du traitement des données. Cela ne constitue en soi pas un changement de fonds, car selon le droit actuel, tout traitement de données doit être licite : base légale pour les traitements effectués par les organes fédéraux (art. 17) ; ne pas porter atteinte de manière illicite à la personnalité des personnes concernées pour les traitements du secteur privé (atteinte reposant sur un motif justificatif) (art. 12 et 13).

En ce qui concerne l'amélioration de la transparence, l'article 4, al. 4 (nouveau) prévoit que la collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée. Cette nouvelle disposition contribue à la réalisation de la motion « Renforcement de la transparence ». Elle constitue une concrétisation du principe de la bonne foi énoncé à l'art. 4, al. 2. Cette exigence de reconnaissabilité existe expressément déjà pour les organes fédéraux lorsqu'ils traitent des données sensibles ou des profils de la personnalité (art. 18, al. 2). Elle est ainsi étendue à tout type de données et s'applique également au secteur privé. Il ne s'agit pas d'un devoir d'information. L'article 4, al. 4 est cependant complété par un devoir d'information à l'art. 7a pour les données sensibles et les profils de la personnalité (voir ci-dessous).

Cette disposition implique que selon le court ordinaire des choses, la personne concernée doit pouvoir percevoir que des données la concernant sont ou vont éventuellement être collectées (principe de prévisibilité). Il doit pouvoir connaître ou identifier la ou les finalités du traitement, soit que selon l'art. 4, 3^{e} al.,

- celles-ci lui sont indiquées à la collecte : par exemple, un assureur énumère dans le formulaire de demande d'un contrat d'assurance les finalités pour lesquelles les données requises vont être traitées ;

- elles découlent des circonstances : par exemple, lorsqu'une personne commande des vêtements auprès d'une entreprise de vente par correspondance, elle communique des informations à cette entreprise en vue de l'exécution de sa commande et notamment pour permettre de lui adresser une facture. Si cette personne ne paye pas la facture, elle doit s'attendre à ce que les données la concernant soient utilisées dans le cadre d'une procédure en recouvrement de dettes ;

- la finalité est prévue par une loi.

Comme cela ressort du message du Conseil fédéral (FF 2003 1915 (1937s.)), les exigences qui devront être remplies pour qu'une collecte soit reconnaissable seront déterminées par les circonstances et conformes aux principes de la proportionnalité et de la bonne foi. Selon la situation, le maître du fichier sera tenu de donner activement l'information à la personne concernée. L'étendue de l'information dépendra également des circonstances. Il faudra ainsi informer activement notamment si les données peuvent être problématiques et si les finalités ne sont pas reconnaissables d'emblée. L'information pourra portée non seulement sur la collecte et les finalités du traitement, mais s'étendre à d'autres éléments déterminants, tel que l'identité du maître du fichier ou les catégories de destinataires des données lorsqu'il est envisagé de communiquer des données. Parfois, il sera nécessaire d'attirer l'attention des personnes sur le caractère facultatif ou obligatoire d'une réponse. Dans d'autres situations, notamment lors de transactions simples, l'information pourra être plus restreinte, voir inutile si le caractère reconnaissable de la collecte et de la finalité du traitement ressort des circonstances ou découle de la loi. Ainsi lorsqu'une personne réserve une chambre d'hôtel et communique à l'hôtelier ses coordonnées et le nombre de nuits qu'il souhaite passer dans l'établissement, il sait en règle générale pourquoi ces données sont traitées. Il n'est pas nécessaire d'informer spécialement. Par contre si l'hôtelier communique ces données à des tiers, la personne concernée est en droit de le savoir.

L'article 4 est complété par un nouvel alinéa 5 qui clarifie la notion de consentement et définit les conditions d'un consentement licite lorsque celui-ci est requis pour le traitement de données personnelles. Il faut d'abord rappeler que le consentement constitue l'un des motifs pouvant justifier le traitement de données personnelles au côté de la loi ou de l'intérêt privé ou public prépondérant. Le LPD

ne prévoit en aucun cas qu'il faille – en particulier dans le secteur privé – faire du consentement une condition préalable à tout traitement et obtenir en particulier le consentement des personnes concernées lorsque le traitement repose sur un autre motif justificatif. La notion de consentement retenue découle de la jurisprudence du Tribunal fédéral et du droit européen, notamment les recommandations du Conseil de l'Europe : le consentement doit être libre et informé. Si le traitement porte sur des données sensibles, il doit en outre être explicite. La personne concernée doit ainsi disposer de tous les éléments du cas d'espèce qui lui permettent de prendre librement sa décision. Elle doit notamment être informée des conséquences et des désavantages qui pourraient résulter pour elle d'un refus. Comme le relève le Conseil fédéral dans son message, « le fait qu'un refus entraîne un désavantage pour la personne concernée n'entache en revanche pas la validité même du consentement, sauf si ce désavantage est sans rapport avec le but du traitement ou qu'il est disproportionné par rapport à celui-ci. Ainsi, la personne qui consent au traitement de données personnelles la concernant pour permettre à un institut financier d'évaluer son crédit en vue de l'obtention d'une carte de crédit consent librement, même si elle sait qu'un refus la privera de la possibilité de se voir délivrer une telle carte. Dans une situation de ce genre, le désavantage qui résulte du non consentement est en effet proportionné au but du traitement. Au contraire, le travailleur contraint de donner son consentement, sous la menace d'un licenciement, à un traitement de données qui n'est pas nécessaire à l'exécution du contrat de travail, n'est pas en mesure de donner son consentement librement. » (FF 2003 1939s)

La modification de l'article 5, 1er alinéa, ne figurait pas dans le projet du Conseil fédéral. Elle porte sur une précision et une atténuation de la portée de l'article 5 qui prévoit l'obligation de celui qui traite des données de s'assurer de leur exactitude. En effet dans sa version actuelle, le principe d'exactitude est formulé de manière trop absolue : « quiconque traite des données personnelles doit s'assurer qu'elles sont correctes ». En réalité, cette formulation ne peut justifier une obligation de ne traiter que des données exactes. Elle exige cependant que l'on s'assure de l'exactitude des données. La portée de cette exigence dépend des conditions propres à chaque traitement de données (notamment finalité du traitement, degré de sensibilité des données, communication à des tiers). Tout en maintenant l'exigence d'exactitude, le texte adopté prévoit ainsi que celui qui traite les données prenne « 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 ». Cette modification statue une obligation de mettre à jour les données lorsque cela est nécessaire. Cette nécessité s'apprécie en fonction du degré de sensibilité des données ou du risque d'atteinte à la personnalité de la personne concernée résultant de l'inexactitude des données traitées. En présence d'un traitement portant sur les préférences concernant certains produits à des fins de marketing, il est moins important de s'assurer que les données sont complètes et à jour que dans celui où le traitement porte sur des données relatives à la solvabilité d'une personne. Une mise à jour est donc nécessaire lorsque l'inexactitude risque de porter atteinte à la personnalité de la personne concernée. Elle ne l'est dès lors pas dans tous les cas. Il n'y aura en règle générale pas d'atteinte à la personnalité si la personne concernée accepte sciemment que des données inexactes soient traitées à son sujet. Ce caractère relatif du principe d'exactitude ressort également de l'article 5, lettre d de la Convention STE 108 et de l'article 6, § 1, lettre d de la directive européenne 95/46/CE sur la protection des données. Le nouveau libellé est proche du libellé de la directive européenne. Il en ressort clairement que l'inexactitude des données peut également résulter du fait que celles-ci sont incomplètes au regard de la finalité pour laquelle elles sont collectées ou traitées.

Communications transfrontières de données (art. 6)

Le régime des flux transfrontières de données a été revu et adapté au protocole additionnel à la Convention STE 108 et dans une certaine mesure au système de la directive européenne 95/46/CE. Le principe de l'interdiction de communiquer des données à l'étranger lorsque la personnalité des personnes concernées est gravement menacée notamment du fait de l'absence d'une protection des données équivalente à celle qui est garantie en Suisse est maintenu. Il est toutefois adapté à la terminologie du protocole additionnel. L'exigence d'équivalence est remplacée par « le niveau adéquat de protection » (du fait de l'absence d'une législation assurant un niveau de protection adéquat). L'obligation de déclarer le transfert d'un fichier à l'étranger lorsque la communication ne découle pas d'une obligation légale et a lieu à l'insu des personnes concernées a été abandonnée d'une part du fait que le nombre de déclarations est resté modeste par rapport aux flux supposés de données au travers des frontières et d'autre part du fait que le préposé n'a pas les ressources nécessaires pour examiner l'ensemble des déclarations avant le transfert des données. Ainsi, seul le devoir de diligence des personnes privées ou des organes fédéraux lors du transfert de données à l'étranger demeure.

La communication de données à l'étranger est possible lorsque plusieurs conditions sont remplies. Tout d'abord la communication doit respecter les principes de base de la protection des données définis aux articles 4, 5 et 7 LPD. La communication des données doit ainsi être licite et reposée sur un motif justificatif, être conforme à la bonne foi et à la proportionnalité, répondre à une finalité déterminée et portée sur des données exactes. Ensuite, la communication n'est en règle générale possible que si le destinataire des données est soumis à une législation assurant un niveau de protection adéquat. Le caractère adéquat du niveau de protection doit être évalué à la lumière de l'ensemble des circonstances relatives au transfert. Le niveau de la protection devrait être évalué au cas par cas et pour chaque transfert ou catégorie de transfert effectué. Dans ce contexte, les circonstances relatives au transfert doivent être examinées et en particulier : la nature des données, les finalités et la durée des traitements pour lesquels les données sont transférées, le pays d'origine et le pays de destination finale, les règles de droit, générales et sectorielles applicables dans l'Etat en question et les règles professionnelles et de sécurité qui y sont respectées.

Une appréciation du caractère adéquat peut toutefois être faite pour l'ensemble d'un Etat permettant ainsi tous les transferts de données vers cette destination. Cela implique en particulier que le destinataire est soumis à une loi offrant un niveau de protection similaire au droit suisse : garantie des droits des personnes concernées (notamment droit d'accès et information), respect des principes de base de la protection des données, autorité de contrôle indépendante. Tel sera le cas en règle générale si l'Etat destinataire est partie à la Convention STE 108 et au protocole additionnel et s'il en remplit les exigences. Le préposé tient une liste des Etats qu'il juge assurer un niveau de protection des données adéquat. Il tient à cet effet également compte des décisions prises par la Commission européenne en application de l'art. 25, § 6 de la directive 95/46/CE.

En l'absence de niveau de protection adéquat, la communication est en règle générale interdite, car elle menace gravement la personnalité des personnes concernées. Toutefois, si celui qui communique les données s'assure, par des moyens adéquats que la transmission des données ne menace pas gravement la personnalité des personnes concernées, il pourra communiquer en l'absence d'une législation assurant un niveau de protection adéquat. L'article 6, 2^{e} alinéa énonce de manière exhaustive 7 conditions alternatives pouvant légitimer une telle communication :

Aux termes de l'article 6, al. 2, let. a, la communication est possible si des garanties suffisantes permettent d'assurer un niveau de protection adéquat à l'étranger. Ces garanties peuvent être prévues

dans un contrat (clauses de protection des données) (voir les différents contrats types élaborés par le Conseil de l'Europe et la Commission européenne, ainsi que le contrat type du PFPDT relatif à l'outsourcing, www.leprepose.ch, rubrique thèmes). Elles peuvent aussi découler d'un code de bonne conduite, c'est-à-dire d'un ensemble de règles auxquelles les personnes privées peuvent se soumettre volontairement. Le système de la sphère de sécurité « Safe Harbor Privacy Framework » (http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_fr.htm) négocié par la commission européenne et les Etats-Unis d'Amérique dans la mesure où l'entreprise américaine destinataire des données s'engage – par écrit - à appliquer les mêmes règles de protection des données aux informations provenant de Suisse que celles qu'elle applique aux données provenant d'un pays de l'Union européenne en application des principes de la sphère de sécurité. Celui qui recourt à de telles garanties demeure responsable de la protection des données. Comme le relève le Conseil fédéral dans son message, il lui incombe de « démontrer qu'il a pris toutes les mesures requises pour s'assurer d'un niveau de protection adéquat. » En outre, conformément à l'al. 3, il doit informer le PFPDT des garanties données (voir ci-dessous).

Aux termes de l'article 6, al. 2, let. b, la communication est également possible dans un cas d'espèce lorsque la personne a donné son consentement. Ce consentement doit être libre et la personne doit avoir été dûment informée (art. 4, al. 5 LPD). Le consentement devra être explicite si la communication porte sur des données sensibles ou des profils de la personnalité. La personne doit ainsi connaître quelles données la concernant vont être communiquées, pour quelles finalités et à quel destinataire. Elle doit être également informée de l'absence d'un niveau de protection adéquat. La communication est limitée à un cas d'espèce, c'est-à-dire qu'elle doit se référer à un cas ou une situation concrète. Il n'est pas possible de donner un consentement global et ainsi autoriser par le biais du consentement de communiquer de manière régulière et systématique des données à l'étranger pour des finalités diverses et des situations différentes. Par contre, la personne concernée peut, dans un cas concret, donner son consentement pour différentes communications lorsque les circonstances de la communication sont pour elle manifestes (FF 1988 II 477). Il doit y avoir manifestation claire de la volonté de la personne d'autoriser la communication.

La communication peut également intervenir si 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). Cette condition est similaire au motif justificatif de l'article 13, al. 2, let. a. La communication doit être indispensable pour la conclusion ou l'exécution du contrat. Par exemple, lors de la conclusion d'un contrat de voyage auprès d'une agence de voyage qui implique la réservation d'un hôtel à l'étranger, l'agence de voyage est légitimée à communiquer les données nécessaires à l'exécution de ce contrat à l'hôtel dans lequel le cocontractant va séjourner.

L'article 6, al. 2., let. d aménage un autre motif pouvant justifier la communication en l'absence d'un niveau de protection adéquat lorsqu'en l'espèce, elle est indispensable soit à la sauvegarde d'un intérêt public prépondérant, soit à la constatation, l'exercice ou la défense d'un droit en justice. La disposition vise à nouveau des situations d'espèce, des cas concrets et ne légitiment pas la communication systématique et régulière de données. Les données communiquées peuvent concerner une personne ou plusieurs personnes et leur communication doit être indispensable, c'est-à-dire sans ces données l'objectif de la communication ne peut pas être atteint. Ainsi, il peut y avoir un intérêt public prépondérant à ce qu'un club de football communique la liste de « supporters violents avérés » afin d'éviter que ces personnes ne mettent en danger la sécurité publique lorsque le dit club doit jouer à l'étranger. De même une personne pourra communiquer des données lorsqu'elle veut faire valoir ses droits à l'encontre d'une tierce personne auprès d'un tribunal d'un pays tiers n'offrant pas un niveau de protection suffisant (par exemple en recouvrement de dette).

L'article 6, al. 2, let. e, autorise la communication de données à l'étranger en l'absence d'un niveau adéquat de protection si elle est, en l'espèce, nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée. La communication est autorisée uniquement si elle tend à protéger un intérêt essentiel pour la vie de la personne concernée. Il s'agit de situations dans lesquelles la personne concernée n'est pas en mesure de faire valoir ses propres intérêts en donnant son consentement et pour lesquelles il peut être présumé de sa part qu'elle aurait donné son accord à la communication. La communication peut à notre avis également porter sur des données de proches de la personne concernée lorsque ceux-ci ne sont pas en mesure de consentir et que sans ces données la vie de la personne concernée est en danger.

La communication est également envisageable lorsque la personne concernée a rendu ses données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement (art. 6, al. 2, let. f).

Enfin l'art. 6, al. 2, let. g, prévoit que la communication à l'étranger peut avoir 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. Cette réglementation permet ainsi la communication transfrontière de données au sein d'un groupe de sociétés. L'existence de règles de protection des données au sein d'une même personne morale ou société ou entre des personnes morales ou sociétés réunies sous une direction unique ne dispense pas ces sociétés du respect des autres dispositions de la LPD, notamment l'information des personnes concernées ou l'exercice du droit d'accès, pour les traitements qu'elles effectuent en Suisse. Ces règles doivent permettre de garantir à l'étranger un niveau de protection adéquat en l'absence d'une législation de protection des données suffisante.

L'article 6, 3^{e} alinéa prévoit en outre que le préposé doit être informé des garanties données (lettre a) et des règles de protection des données (lettre g). Le Conseil fédéral règle les modalités du devoir d'information. Ce devoir d'information n'implique pas que le préposé donne son accord à ces garanties ou à ces règles de protection des données. Il donne cependant la possibilité au préposé d'examiner le cas échéant si ces garanties ou ces règles sont suffisantes pour assurer un niveau de protection des données adéquat en l'absence d'une législation équivalente (art. 26, let. e LPD). S'il constate des insuffisances, il pourra demander d'y remédier et éventuellement émettre une recommandation (art. 27 et 29 LPD). Si les clauses de protection des données se basent sur des contrats ou des règlements modèles émis par le préposé ou qu'il a reconnu, le préposé ne procédera pas à examen ; toutefois, le maître du fichier devra l'informer qu'il recourt à de telles garanties (art. 5, 3^{e} al. OLPD-Rev). Il ne sera également pas nécessaire d'informer sur les garanties ou les règles de protection des données lors de chaque communication. Il n'y a pas lieu de renouveler l'information aussi longtemps qu'après avoir informé le préposé, le responsable du traitement utilisent les mêmes garanties lors de la communication pour autant que les catégories de destinataires, les finalités du traitement ou les catégories de données communiquées restent inchangés. Il en va de même pour des communications selon la lettre g dans la mesure où elles sont effectuées au sein d'une même personne morale ou société ou entre des personnes morales ou sociétés réunies sous une direction unique aussi longtemps que les règles de protection des données demeurent inchangées. Le PFPDT publiera en outre une liste des contrats modèles qui peuvent être utilisés.

Information des personnes concernées (article 7a)

L'article 7a prévoit l'obligation pour tout maître de fichier qui collecte des données sensibles ou des profils de la personnalité d'en informer la personne concernée. Cette obligation existe non seulement lorsqu'il collecte les données directement auprès de la personne concernée, mais aussi lorsqu'il les collecte auprès de tiers. Ce devoir d'information réalise la motion 00.300 de la Commission des affai-

res juridiques du Conseil des Etats « renforcement de la transparence lors de la collecte de données personnelles ». Elle permet également un rapprochement avec la législation européenne et notamment la directive européenne 95/46/CE ou les recommandations du Conseil de l'Europe. Toutefois, le nouvel article 7a se distingue des textes européens en limitant le devoir d'information aux données sensibles ou aux profils de la personnalité. Les textes européens vise toute collecte de données personnelles quelque soit la nature de ces données. Même limité, ce devoir d'information renforce cependant la position des personnes concernées qui pourront plus aisément et plus rapidement faire valoir leur droit, voire s'opposer à un traitement qui ne leur parait pas justifié. Il oblige également les maîtres de fichier à se montrer plus vigilant et à s'abstenir de collecter et de traiter des données sensibles ou des profils de la personnalité dont il n'a pas absolument besoin pour remplir ses tâches.

L'article 7a, 2e alinéa, détermine l'étendue du devoir d'information. L'information doit portée sur toutes les informations pertinentes pour que la personne concernée soit en mesure de se faire une idée sur le traitement et le cas échéant faire valoir ses droits. Comme le relève le Conseil fédéral dans son message (FF 2003 1943), « le maître du fichier doit – en règle générale de manière explicite – fournir à la personne concernée toutes les informations nécessaires pour que le traitement soit conforme aux principes de la bonne foi et de la proportionnalité. Ainsi la personne concernée doit au minimum connaître l'identité du maître du fichier, les finalités du traitement pour lequel les données sont collectées et les catégories de destinataires des données si leur communication est envisagé (al. 2, let. a – c). Si d'autres informations sont nécessaires pour éclairer la personne concernée, le maître du fichier, conformément au principe de la bonne foi, doit les communiquer à la personne concernée. Par exemple, il peut s'avérer utile de lui préciser si la collecte est obligatoire ou revêt un caractère facultatif, voire de l'informer sur les conséquences d'un refus de répondre à certaines questions.

Lorsque la collecte n'intervient pas auprès de la personne concernée, celle-ci doit néanmoins en être informée. L'information doit intervenir au plus tard lors de l'enregistrement des données ou s'il n'y a pas d'enregistrement, lors de leur première communication à un tiers (art. 7a, al. 3). Dans ce dernier cas, il est souhaitable de donner l'information avant de communiquer les données pour permettre à la personne concernée de réagir, notamment si leur communication n'est pas obligatoire.

Le maître du fichier n'est tenu d'informer les personnes concernées que dans la mesure où celles-ci n'ont pas déjà été informées (art. 7a, al. 4). L'information peut avoir été délivrée antérieurement par le maître du fichier ou avoir été donnée à la personne concernée par un tiers. Ainsi, si le maître du fichier a informé la personne concernée lors d'une première collecte, il n'a pas besoin de renouveler l'information à chaque nouvelle collecte, à moins que les circonstances du traitement changent, notamment que les données soient collectées pour des finalités différentes que celles communiquées antérieurement.

Le maître du fichier n'est également pas tenu d'informer lorsque l'enregistrement des données ou leur communication sont expressément prévus par la loi (art. 7a, al. 4, let. a) ou lorsque le devoir d'information est impossible à respecter ou nécessite des efforts disproportionnés (art. 7a, al. 4, let. b), par exemple lorsque le maître du fichier n'a pas la possibilité de contacter la personne concernée. Le maître du fichier doit néanmoins entreprendre les démarches qu'on peut attendre raisonnablement de lui, compte tenu des circonstances. « Il ne peut se contenter de présumer que l'information est impossible ou disproportionnée. Son comportement doit être examiné conformément au principe de la bonne foi. » (FF 2003 1944).

Le maître du fichier peut également refuser ou restreindre l'information, voire en différer l'octroi lorsque l'une des conditions de l'article 9 est remplie, à savoir :

- lorsqu'une loi au sens formel le prévoit (al. 1, let. a)
- lorsque les intérêts prépondérants d'un tiers l'exigent (al. 1, let. b)
- s'il s'agit d'un organe fédéral, lorsqu'un intérêt public prépondérant l'exige (al. 2, let a) ou l'information risque de compromettre une instruction pénale ou une procédure d'instruction (al. 2, let b)
- s'il s'agit d'un maître de fichier privé, lorsque ses intérêts prépondérants l'exigent et à condition qu'il ne communique pas les données personnelles à des tiers (al. 3).

Contrairement au refus de donner des renseignements lorsque la personne exerce son droit d'accès (art. 8, resp. 9, al. 4, LPD), le maître du fichier n'a pas à motiver le fait qu'il refuse, restreigne ou diffère l'octroi des informations. Contrairement au projet du Conseil fédéral, le Parlement n'a pas voulu prescrire une obligation d'information une fois le motif de restriction disparu. Cependant, en cas de refus ou de restriction, il est recommandé, dans la mesure où cela s'avère possible et non disproportionné, d'informer la personne concernée dès que les motifs de restriction ont disparu.

La LPD ne prescrit également aucune forme sur la manière d'informer. Il n'est pas nécessaire de remettre une information écrite à la personne concernée ; elle peut être informée oralement. A des fins de preuve, il est recommandé néanmoins d'utiliser la forme écrite. En effet, celui qui intentionnellement ne respecte pas son obligation d'information peut sur plainte être puni des arrêts ou de l'amende (art. 34, al. 1, let. 1). La forme de l'information doit être également appropriée aux circonstances. Elle peut notamment intervenir sous forme de publication, d'affiche, de prospectus, être intégrée dans des conditions générales, dans une correspondance adressée aux personnes concernées ou annexée à un contrat ou à une facture. Elle peut également figurer sur la page d'accueil d'un site internet. Il est important d'assurer la visibilité de l'information et de la donner de manière intelligible et lisible. Le maître du fichier peut ainsi lier l'octroi de l'information avec la poursuite d'un autre objectif. Ainsi par exemple, « si la communication des données personnelles à des tiers est envisagée et que cette communication n'est ni obligatoire ni nécessaire à l'exécution d'un contrat, l'attention de la personne concernée peut être attirée au moyen d'une clause par laquelle elle est invitée à autoriser ou à refuser la communication : ce mode de faire permet au maître du fichier de s'assurer que la personne concernée a reçu l'information et n'entend pas s'opposer ultérieurement à la communication des données. » (FF 2003 1043s).

Les maîtres de fichier disposeront d'un délai d'une année à partir de l'entrée en vigueur de la loi pour mettre en œuvre les mesures d'information nécessaires (dispositions transitoires). Le devoir d'information ne vaut pas pour les données qui ont été collectées avant l'entrée de la LPD-Rev à moins que de nouvelles données soient recueillies en relation avec un traitement existant ou qu'une personne n'était pas encore concernée par le dit traitement.

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

L'article 10a règle le traitement de données personnelles sur mandat. Cette disposition reprend l'actuel article 14 et étend son champ d'application aux organes fédéraux. Le traitement sur mandat ordonné par un organe fédéral n'était pas réglé expressément dans la LPD, mais à l'article 22 OLPD. Par rapport au droit en vigueur, l'article 10a précise d'une part qu'un traitement ne peut être confié à un tiers que si une convention ou une loi le prévoit. D'autre part, le mandataire doit garantir la sécurité des données, c'est-à-dire prendre des mesures techniques et organisationnelles appropriées afin de protéger les données personnelles de tout traitement non autorisé. S'il n'est pas prévu dans une loi, le

traitement par un tiers doit faire l'objet d'une convention (contrat) entre le responsable du traitement (mandant) et le tiers appelé à traiter les données (mandataire). Cette convention devra fixer les obligations du mandataire, notamment l'étendue du traitement et les exigences de sécurité. Le mandant demeure responsable de la protection des données et il répond du préjudice qu'il peut avoir causé en confiant le traitement à un tiers, notamment s'il ne s'est pas assuré de la sécurité des données (voir aussi 9ème Rapport d'activités 2001/2002, p. 37ss).

Procédure de certification (art. 11)

L'article 11 (nouveau) est une norme incitative qui constitue un premier pas vers l'auto réglementation, comme instrument complétant ou concrétisant les exigences de la loi. Aux termes de cette disposition, les fournisseurs de systèmes de logiciels et de traitement des données, ainsi que les personnes privées ou les organes fédéraux qui traitent des données personnelles peuvent soumettre leurs systèmes, leurs procédures et leur organisation à une évaluation effectuée par des organismes de certification agréés et indépendants. L'objectif est d'améliorer la protection et la sécurité des données. Cette certification peut se faire sur des produits (logiciels ou matériels) ou sur des traitements. Elle permet de concrétiser pratiquement les dispositions légales en développant des produits et des systèmes conformes aux exigences de protection des données. Elle permet également de tenir compte des évolutions technologiques. Lorsqu'au terme de la procédure de certification, l'organisme certifiant parvient à la conclusion que les normes légales et techniques sont respectées, il délivre un label de qualité (label de protection des données). Les personnes privées ou organes fédéraux qui auront obtenu une certification seront dispensés d'annoncer les fichiers objets de la certification (art. 11a, al. 5, let. f). La procédure d'accréditation des organismes de certification, les conditions de la procédure de certification et les conditions d'octroi du label de qualité feront l'objet d'une ordonnance spécifique. Si le PFPDT n'est ni organe d'accréditation, ni organe de certification, il est néanmoins appelé à jouer un rôle important dans la mise en place de cet instrument, notamment en examinant les procédures de certification et en émettant le cas échéant des recommandations (art. 31, al. 1, let. f). Le service d'accréditation suisse l'associera également à la procédure d'accréditation et au contrôle (art. 2 P-OCPD). Le PFPDT devra également reconnaître les organismes de certification étrangers voulant exercer en Suisse (art. 3 P-OCPD).

Registre des fichiers (art. 11a)

La révision maintient le registre des fichiers, comme élément de la transparence des traitements et outil devant permettre aux personnes concernées de faire usage des droits que leur confèrent la loi. Si aujourd'hui la visibilité du registre est insuffisante du fait notamment de ressources insuffisantes qui empêchent d'assurer régulièrement sa publication, la révision prévoit d'améliorer la situation en rendant le registre accessible en ligne (publication sur Internet). En outre, la procédure d'annonce sera allégée en offrant aux maîtres de fichiers une possibilité d'annoncer leur fichier en ligne. Ce système sera d'abord disponible pour l'administration fédérale, mais devrait rapidement être accessible aux personnes privées.

Les exigences d'une meilleure transparence des traitements (art. 4, al. 4, art. 7a) ont également des conséquences sur l'obligation d'annonce des fichiers. Si les organes fédéraux demeurent tenus de déclarer tous leurs fichiers, l'obligation d'annonce dans le secteur privé devient plus étendue. En effet à l'avenir, le maître de fichier devra annoncer un fichier lorsqu'il traite régulièrement des données sensibles ou des profils de personnalité ou lorsqu'il communique régulièrement des données personnelles à des tiers, même si la personne concernée a connaissance du traitement. Il en résulte que des fichiers qui ne devaient pas être déclarés avant l'entrée en vigueur de la révision devront être décla-

rés. Bien que la révision ne le prévoie pas expressément, le PFPDT accordera un délai d'une année au maître du fichier pour se mettre en conformité avec les nouvelles obligations (art. 38 LPD par analogie). Les fichiers doivent être déclarés avant d'être opérationnels (art. 4, al. 4).

Toutefois, la loi énonce une série d'exceptions à l'obligation d'annonce (art. 11a, al. 5). Ces exceptions peuvent être invoquées aussi bien par les organes fédéraux que par les personnes privées. Ainsi, il n'y a pas lieu d'annoncer un fichier lorsque :

- la personne privée traite des données en vertu d'une obligation légale ;
- le Conseil fédéral a désigné le traitement comme n'étant pas susceptible de menacer les droits des personnes concernées. Ces fichiers ou traitements sont énoncés dans l'ordonnance aux articles 4 et 18 OLPD-Rev ;
- le maître de fichier utilise exclusivement le fichier pour la publication dans la partie rédactionnelle d'un média à caractère périodique et ne communique pas les données à des tiers à l'insu des personnes concernées. Cette exception n'est pas nouvelle. Elle figurait à l'art. 4 OLPD ;
- Les données sont traitées par un journaliste qui se sert du fichier comme un instrument de travail personnel. Cette exception figurait également à l'art. 4 OLPD ;
- 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. Cette exception se veut également un encouragement à l'auto réglementation. L'institution de conseiller à la protection des données au sein des entreprises ou des administrations publiques est également prévu par la directive européenne 95/46/CE. Cette institution est déjà pratiquée dans plusieurs pays, notamment l'Allemagne, la France, les Pays-Bas et la Suède et est jugée positive non seulement par les autorités de protection des données, mais également par les entreprises ou les administrations qui y recourent. Pour pouvoir bénéficier de l'exception, le conseiller doit pouvoir exercer ses tâches de manière indépendante et avoir les moyens suffisants pour accomplir ses tâches que relèvent du conseil, de la formation, de la sensibilisation et du contrôle. Il doit avoir une position dans l'entreprise qui lui permette d'exercer sa tâche sans pression et qui ne le mette pas en conflit avec l'accomplissement d'autres tâches. Il ne serait ainsi pas concevable que ce conseiller soit également responsable de la gestion du personnel. Il doit également avoir les connaissances professionnelles nécessaires à l'accomplissement de sa tâche. Il ne doit également pas subir de pression de son employeur quant à la manière de mener sa tâche ni être discriminé du fait de l'accomplissement de sa mission ;
- le maître du fichier s'est soumis à une procédure de certification au sens de l'art. 11, a obtenu un label de qualité et a annoncé le résultat de la certification au préposé .

La liste des maîtres de fichiers qui sont déliés de leur devoir de déclaration sera publiée.

Traitement de données personnelles par des personnes privées

Dans le secteur privé, le traitement de données personnelles est possible aussi longtemps qu'il ne porte pas une atteinte illicite à la personnalité des personnes concernées. Le traitement des données doit en particulier respecter les principes généraux du traitement définis aux articles 4 et suivants et dans la mesure où il y a atteinte à la personnalité, l'atteinte doit reposer sur un motif justificatif (art. 13 LPD : loi, consentement, intérêt public ou privé prépondérant).

La révision de la LPD apporte une clarification en modifiant l'article 12, al. 2. Dans sa version actuelle, l'article 12 stipule que personne n'est en droit, sans motif justificatif, notamment de traiter des données personnelles en violation des principes définis aux art. 4 et suivants (let a), de traiter des données contre la volonté expresse de la personne concernée (let b) ou de communiquer à des tiers des données sensibles ou des profils de la personnalité (let c). Pris à la lettre, cette disposition laisse supposer que sur la base d'un motif justificatif, il est possible de traiter des données en violation du principe de la bonne foi, de manière illicite ou disproportionnée, qu'il est possible de traiter des données fausses ou de renoncer à prendre des mesures techniques et organisationnelles pour éviter que des tiers non autorisés puissent avoir accès à ces données. Une telle interprétation était choquante et ne correspondait pas à la pratique et à l'esprit de la loi. Tout au plus était-il légitime de concevoir une possibilité de déroger à l'article 4, al. 3 (finalité). Le nouvel article 12, 2e al. prévoit désormais explicitement qu'il n'est pas possible de traiter des données en violation des principes des articles 4 et suivants, y compris concernant le principe de finalité. Par rapport au principe de finalité, cela est justifié par le renforcement de la transparence des traitements (art. 4. al. 5 et art. 7a).

Certains estiment à tort que cette clarification empêchera à l'avenir certains traitements. Ainsi, une assurance peut proposer à un assuré de conclure au côté de sa police d'assurance maladie complémentaire une assurance vie et pour se faire d'utiliser les données qu'elle détient déjà au sujet de cet assuré dans la mesure où la personne concernée donne son consentement ou le traitement repose sur un autre motif justificatif. Dans un tel cas, nous serons en présence d'un nouveau traitement et d'une nouvelle finalité. La collecte et en particulier la finalité du traitement doivent être reconnaissable pour la personne concernée. Une information active sera nécessaire si des données sensibles ou des profils de la personnalité sont collectées, ce qui sera le cas dans le domaine de l'assurance vie (voir aussi Notice interprétative de l'Office fédéral de la justice, janvier 2007, http://www.bj.admin.ch/etc/medialib/data/staat_buerger/gesetzgebung/datenschutz.Par.0020.File.tmp/20070111-Auslegungshilfe-f.pdf).

Traitement des données par des organes fédéraux

Organe responsable et contrôle (art. 16, al. 2)

L'article 16, al. 2 précise les compétences du Conseil fédéral lors de traitement conjoint de données personnelles. Le Conseil fédéral pourra non seulement régler la responsabilité des différents organes impliqués, mais également les procédures de contrôle à mettre en place pour garantir le respect des dispositions de protection des données. Il pourra notamment exiger qu'un organe fédéral qui confie un traitement à un tiers ou qui traite conjointement des données avec des personnes privées ou des organes cantonaux vérifient les conditions de sécurité avant de donner des accès à des informations sensibles.

Bases juridiques

L'article 17, al 2 a été légèrement modifié. Tout d'abord à la lettre b, il est précisé que l'autorisation délivrée par le Conseil fédéral pour le traitement de données sensibles ou de profils de la personnalité en l'absence de base légale ne peut concerner qu'un cas d'espèce et ne doit pas porter sur des traitements portant sur un nombre indéterminé de cas. Cette précision correspond à l'interprétation qui a été donnée de cette disposition.

Ensuite à la lettre c, à l'instar de l'art. 12, al. 3, on tient compte du droit des personnes concernées de s'opposer au traitement même lorsqu'elle a rendu ses données accessibles à tout un chacun. Ainsi, l'organe fédéral peut exceptionnellement, en l'absence de base légale formelle, traiter des données sensibles ou des profils de la personnalité que la personne concernée a rendues accessibles à tout un chacun pour autant qu'elle ne se soit pas formellement opposée à leur traitement. L'opposition doit être clairement signifiée de manière à ce qu'il n'y ait pas de doute sur la volonté de la personne concernée.

Traitement de données automatisé dans le cadre d'essais pilotes (art. 17a)

L'article 17a aménage une autre exception à l'exigence d'une loi au sens formel pour le traitement de données sensibles ou de profils de la personnalité. Il s'agit d'une norme « transitoire » qui permet au Conseil fédéral d'autoriser la mise en œuvre de tel traitement avant l'adoption des bases légales nécessaires si une phase d'essai est absolument indispensable pour la mise en œuvre technique d'un traitement déterminé ou d'un système informatique. Cela doit permettre d'évaluer tous les besoins liés au traitement, de déterminer plus précisément le cercle des ayants-droits et d'éviter de mettre en place des bases légales imprécises ou rapidement dépassées car ne correspondant pas à la réalité.

Le recours à cette clause d'exception n'est possible que si trois conditions cumulatives sont remplies :

- les tâches qui nécessitent le traitement des données sensibles ou de profils de la personnalité sont réglées dans une loi au sens formel ;
- des mesures appropriées doivent être prises aux fins de limiter les atteintes à la personnalité ;
- la mise en œuvre du traitement rend indispensable une phase d'essai avant l'entrée en vigueur de la loi au sens formel.

L'alinéa 2 énoncent les critères qui permettent de déterminer si une phase d'essai est indispensable :

- l'accomplissement des tâches nécessite l'introduction d'innovations techniques dont les effets doivent être évalués. « Tel est notamment le cas lorsqu'un logiciel déterminé n'a pas encore été testé ou utilisé avec des données réelles ou lorsque de nouvelles techniques pour la saisie et la transmission d'informations doivent être introduites (par exemple un système de lecture automatisée des numéros d'immatriculation des véhicules) » (FF 2003 1954) ;
- l'accomplissement des tâches nécessitent la prise de mesures organisationnelles ou techniques importantes dont l'efficacité doit être examinée, notamment dans le cadre d'une collaboration entre les organes fédéraux et le cantons. On peut citer la mise en place d'une banque de données concernant des profils ADN qui nécessite de définir précisément les flux d'informations ou les rôles des différents acteurs pour garantir de manière optimale la protection des personnes concernées ;

- le traitement exige que des données sensibles ou des profils de la personnalité soient rendues accessibles aux autorités cantonales en ligne. Cela permet de vérifier la pertinence d'un tel accès, notamment quant à sa fréquence d'utilisation.

Avant d'autoriser une telle phase d'essai, le Conseil fédéral doit consulter le préposé fédéral. En fait, le devoir de consultation incombe à l'organe responsable du traitement. Il doit en particulier informer le PFPDT sur la manière dont il a prévu d'assurer que les exigences de l'art. 17a LPD seront remplies. Aux termes de l'art. 26a OLPD-Rev , il remet au PFPDT tous les documents nécessaires et en particulier un descriptif général de l'essai pilote, un rapport démontrant la nécessité de l'essai et du traitement de données sensibles ou des profils de la personnalité, le projet d'ordonnance, des informations sur les mesures techniques et organisationnelles et des informations sur la planification de l'essai pilote. Sur cette base, le PFPDT émet un avis, lequel ne lie pas le Conseil fédéral. Il ne devrait cependant pas passer outre l'avis du préposé à moins que des circonstances particulières le justifient (FF 2003 1954). La phase d'essai est limitée dans le temps. L'organe fédéral responsable doit adresser un rapport d'évaluation au Conseil fédéral au plus tard deux ans après la mise en œuvre. Il doit notamment proposer la poursuite ou l'interruption du traitement (al. 4). En particulier, il conviendra de tirer un bilan complet de l'essai en examinant non seulement les avantages de la solution, mais également les désavantages. Le traitement doit en tous les cas être interrompu si aucune loi au sens formel le régissant n'est entrée en vigueur dans un délai de cinq ans à partir de la mise en œuvre de l'essai pilote (al. 5).

Collecte des données personnelles (art. 18)

L'introduction du nouvel art. 4, al. 4 (collecte reconnaissable) a pour conséquence que l'art. 18, al. 2 a été biffé. L'exigence de reconnaissabilité couvre toutes les données personnelles indépendamment de leur nature.

Communication des données (art. 19)

L'article 19 a été modifiée d'une part pour tenir compte de la définition du consentement donnée à l'article 4, al. 5 : à l'avenir le consentement ne peut être présumé (art. 19, al. 1, let. b). D'autre part à l'instar de l'art. 17, al. 2, let, c, la communication de données que la personne concernée a rendu accessible à tout un chacun, n'est possible que pour autant que la personne concernée ne s'y soit pas formellement opposée.

L'article 19 a également été modifiée avec l'adoption de la loi fédérale sur le principe de la transparence dans l'administration (LTrans). L'article 7 LTrans prévoit en outre qu'exceptionnellement des documents officiels peuvent être rendus accessibles même si leur divulgation porte atteinte à la sphère privée de tiers. Dans un tel cas, l'intérêt public à la transparence doit l'emporter sur l'intérêt à la protection de la sphère privée. L'article 9, al. 2 LTrans prévoit que l'accès à des données personnelles est régi par la LPD. Dans ce cas, c'est l'article 19 LPD qui s'applique et en particulier l'article 19, al. 1bis (nouveau). Cette disposition vise à établir un équilibre entre les exigences de la protection des données et le principe de transparence de l'administration. Ainsi, aux termes de la nouvelle disposition, les organes fédéraux peuvent communiquer des données personnelles dans le cadre de l'information officielle du public, d'office ou suite à une demande basée sur la Ltrans lorsque les données concernées sont en rapport avec l'accomplissement de tâches publiques et que la communication répond à un intérêt public prépondérant. Il convient d'examiner de cas en cas les données qui peuvent être ainsi communiquées en procédant à une évaluation des intérêts en présence. Ainsi aux termes du message du Conseil fédéral (FF 2003 1873), la communication « ne doit pas être incompa-

tible avec l'objectif en vue duquel les données ont été procurées à l'origine (cf. art. 4, al. 3, LPD). L'information par les autorités peut, dans certaines conditions du moins, être considérée comme étant compatible avec le principe de la LPD concernant la finalité du traitement, puisque l'obligation d'informer est formellement prévue dans une loi. Il y a lieu en particulier d'examiner si la personne concernée a fourni librement des données la concernant ou si elle avait une obligation légale de le faire ; il convient également de tenir compte de la nature des données et des conséquences que leur accès pourrait avoir sur la personne concernée. (...) Il convient également de se référer au principe de la finalité du traitement pour établir si les données personnelles à communiquer sont en rapport avec l'accomplissement de tâches publiques. » Selon l'article 19, al. 3bis LPD, un organe fédéral peut aussi rendre accessible des données à un tout un chacun (information active) au moyen de services d'information et de communication automatisés, par exemple par le biais d'Internet, lorsqu'une base légale prévoit la publication des données ou lorsque l'organe fédéral a rendu des données accessibles sur la base de l'article 19, al. 1bis. Cette possibilité est cependant limitée dans le temps. Ainsi dès que l'intérêt public ayant justifié la publication a disparu, les données doivent être retirées ou effacées. Cela permet notamment d'éviter que des données non actuelles puissent être consultées et traitées. L'accès aux données doit être prévu de manière à respecter le principe de proportionnalité, par exemple en limitant l'accès à un cercle déterminé de personnes. En outre, pour éviter que les données puissent aisément être transférées dans d'autres bases de données, il conviendrait de concevoir les systèmes d'information de manière à ce qu'ils ne soient pas accessibles au moteur de recherche.

Préposé fédéral à la protection des données et à la transparence

Avec l'entrée en vigueur de la LTrans, le préposé s'est vu attribuer de nouvelles tâches. Il doit en particulier assurer la médiation entre l'organe fédéral qui refuse une demande d'accès à des documents officiels et le demandeur ou entre l'organe fédéral et une personne concernée dont les données devraient être communiquées à un tiers qui en fait la demande (art. 13, 18 LTrans). Dans le cadre de la LTrans, il est également autorité de conseil et doit informer les particuliers ou les autorités sur les modalités d'accès à des documents officiels. Il sera amener à prendre également position sur les projets législatifs fédéraux ou les mesures de la Confédération qui touchent fondamentalement au principe de la transparence (art. 18). Enfin, il devra faire rapport au Conseil fédéral et notamment procéder régulièrement à une évaluation de l'application, de l'efficacité et des coûts engendrés par la mise en œuvre de la LTrans.

La révision de la LPD apporte également quelques modifications dans les compétences du PFPDT (voir art. 29, al. 2, let. c, art. 31, al. 1, let d à g). En particulier, il pourra à l'avenir également recourir auprès du tribunal administratif fédéral contre les décisions de la Chancellerie fédérale ou des départements fédéraux qui ne donnent pas suite à une recommandation émise à l'encontre d'un organe fédéral (art. 27, al. 6 LPD).

Dispositions finales

Traitement de données par des organes cantonaux (art. 37)

La LPD n'est pas applicable aux traitements effectués par des organes cantonaux sauf si un canton ne dispose pas de dispositions de protection des données et traitent des données en exécution du droit fédéral. Par rapport au droit actuel, la révision renforce les exigences à l'égard des cantons. Les traitements de données personnelles en exécution du droit fédéral doivent non seulement être soumis

à des dispositions cantonales de protection des données pour ne pas être soumis au droit fédéral, mais ces dispositions doivent également assurer un niveau de protection adéquat. Un niveau sera adéquat s'il est conforme aux exigences de la Convention 108 et du protocole additionnel (FF 2003 1957).