Commentaire de l'Office fédéral de la justice à l'appui de l'ordonnance du 14 juin 1993 (état au 1er janvier 2008) relative à la loi fédérale sur la protection des données (OLPD, RS 235.11)

1. Champ d'application

L'ordonnance ne contient pas de disposition particulière relative à son champ d'application. Celui-ci est défini par l'article 2 de la loi fédérale du 19 juin 1992 sur la protection des données (LPD). Une précision cependant: l'ordonnance ne s'applique pas directement aux cantons lorsque ceux-ci, conformément à l'article 37 LPD, sont soumis à la loi fédérale sur la protection des données. Il revient en effet aux cantons de prévoir les dispositions d'application compte tenu de leur autonomie d'organisation. Toutefois, ils sont libres de s'inspirer de la présente ordonnance et peuvent le cas échéant l'appliquer par analogie.

2. Structure de l'ordonnance

La présente ordonnance se divise en 4 chapitres:

1. le traitement de données personnelles par des personnes privées (chapitre 1)
2. le traitement de données personnelles par des organes fédéraux (chapitre 2)
3. le registre des fichiers, le Préposé fédéral à la protection des données et à la transparence (ci-après préposé) et la procédure devant le Tribunal administratif fédéral (chapitre 3)
4. les dispositions finales (chapitre 4).

Cette structure tient compte du fait que la loi fédérale s'applique aussi bien aux traitements de données personnelles effectués par des personnes physiques ou juridiques de droit privé qu'à ceux entrepris par les organes fédéraux. Bien que les dispositions régissant ces deux secteurs ne soient pas foncièrement différentes, il paraît opportun de bien distinguer les deux secteurs en regroupant en des chapitres spécifiques les dispositions qui les régissent. Toutefois, afin d'éviter de trop fréquentes répétitions, le chapitre régissant les organes fédéraux contient des renvois au chapitre relatif au secteur privé.

3. Droit d'accès (art. 1 et 2, 13 et 14 OLPD)

3.1 Modalités (art. 1 et 13)

Le droit d'accès est une institution fondamentale du droit de la protection des données. Sans droit d'accès, la personne concernée ne serait pas en mesure de faire valoir effectivement ses prétentions en matière de protection des données et en particulier de savoir si des données la concernant sont traitées, d'en prendre connaissance et si nécessaire de les faire corriger ou détruire. La LPD règle de manière détaillée l'exercice du droit d'accès par les personnes concernées, son étendue et les restrictions qui peuvent y être apportées.

La loi cependant ne règle pas toutes les modalités d'exercice du droit d'accès. Elle confère cette compétence au Conseil fédéral, lequel peut également prévoir des exceptions aux principes de la gratuité et de l'octroi des renseignements demandés en la forme écrite.

Les articles 1 et 13 de l'ordonnance règlent donc les modalités d'exercice du droit d'accès, à savoir:

- La manière d'introduire une demande d'accès: la personne concernée doit le faire par écrit et justifier de son identité, notamment en joignant une photocopie de sa carte d'identité. Elle n'a pas à produire une pièce d'identité si elle peut être identifiée d'une manière différente. Ainsi, il va sans dire que si la personne concernée est connue du maître du fichier, elle n'a pas à justifier plus avant de son identité.

- De même, la forme écrite n'est pas toujours requise. Dans certains cas, par exemple lors de demande de consultation d'un dossier du personnel, la forme orale peut suffire. Il revient au maître du fichier de décider s'il exige néanmoins la forme écrite. D'aucuns auraient souhaité que l'ordonnance limite l'exercice du droit d'accès en exigeant de la personne concernée qu'elle motive sa demande et indique précisément le fichier dont elle souhaite obtenir des informations. Une telle limitation serait contraire à la LPD. Toutefois, dans la mesure où la personne concernée en a connaissance, elle devrait indiquer le nom du fichier et le genre de données afin de faciliter les recherches du maître de fichier.
- Les renseignements sont en principe fournis par écrit, sous forme d'imprimé ou de photocopie (art. 8, al. 5, 1ère phrase LPD). La forme écrite couvre non seulement les données requises, y compris les informations disponibles sur l'origine des données, mais également les indications relatives au but et à la base juridique du traitement, ainsi qu'aux catégories de données personnelles traitées, de participants au fichier et de destinataires des données (art. 8, al. 2, let. b, LPD). Toutefois, le maître du fichier peut autoriser ou proposer à la personne concernée de venir consulter ses données sur place (art. 1, al. 3 OLPD). Une telle procédure est plus économique et plus rationnelle, lorsque les données sont réparties dans différents fichiers ou dossiers, qu'elles ont une ampleur particulière ou qu'elles sont conservées sous des formes différentes (par exemple, une banque de données multimédias comprenant des données sous forme de texte, d'images ou de son). De même, on peut recourir à cette procédure lorsque des explications doivent accompagner l'octroi des renseignements demandés. Lors d'une consultation sur place, la personne concernée doit néanmoins avoir la possibilité de demander une photocopie de certaines pièces de son dossier. Un tel droit n'est pas sans importance, en particulier lors de la consultation de son dossier du personnel. Les renseignements peuvent également être donnés par oral, par exemple par téléphone. Toutefois, une telle pratique ne peut être envisagée que lorsque les renseignements fournis ne portent pas sur des données sensibles et lorsqu'il s'agit de renseignements relativement peu étendus. On ne peut recourir à cette procédure que si la personne concernée y a consenti et pour autant qu'elle ait été formellement identifiée.
- L'article 1 alinéa 2 prévoit également que la demande d'accès et la communication de renseignements peuvent être faites par voie électronique à condition que certaines exigences soient respectées.
- Tout d'abord des mesures adéquates doivent être prises afin de s'assurer que la personne qui fait valoir son droit d'accès est la personne concernée. En effet le maître du fichier doit vérifier que le demandeur est la personne dont les données sont traitées. Tel sera le cas par exemple lorsque la personne concernée utilise une signature électronique (voir notamment la loi fédérale sur la signature électronique, RS 943.03). Conformément à la terminologie de la sécurité informatique, il ne s'agit donc pas à proprement parler d'une identification, mais d'une authentification. Toutefois pour respecter la terminologie de la disposition et ne pas introduire une nouvelle notion, qui de surcroît n'est pas connue de tous, le terme «identifier» a été préféré à celui d' «authentifier» (art. 1, al. 2, let. a).
- Les données de la personne concernée doivent en outre être protégées de manière adéquate de tout accès non autorisé par un tiers (art. 1, al. 2, let. b). Il s'agira donc de coder les messages électroniques ou d'installer un accès Internet sécurisé lorsque la personne concernée peut accéder en ligne à ses données personnelles. Cette disposition vise avant tout le secteur privé. Il n'est toutefois pas exclu qu'elle puisse un jour également concerner le secteur public. La question de savoir si les mesures sont adéquates dépend des circonstances du cas d'espèce. Les exigences seront plus élevées s'il s'agit de données sensibles ou de profils de la personnalité que pour les autres données personnelles.
- Les renseignements doivent être donnés dans les 30 jours suivant la réception de la demande (art. 1, al. 4). Si le maître du fichier n'est pas en mesure de le faire, il doit en informer la personne concernée en lui indiquant le délai dans lequel interviendra la réponse. Le droit d'accès n'a de sens que si la personne concernée peut rapidement obtenir satisfaction, surtout lorsque les données font l'objet de réactualisations fréquentes. Lorsque les renseignements sont

refusés, limités ou différés, le maître du fichier en informe également l'intéressé dans les 30 jours et lui indique les motifs.

- Lorsque plusieurs maîtres du fichier gèrent en commun un ou des fichiers, le droit d'accès peut être exercé à l'encontre de chacun d'eux sauf si l'un d'eux a été désigné responsable du traitement de l'ensemble des demandes de renseignements (*art. 1, al. 5)*. Afin de faciliter la procédure et d'éviter que la personne concernée doive déposer plusieurs demandes d'accès, chaque maître du fichier interpellé donne des renseignements pour son seul domaine d'activité. Lorsqu'un maître de fichier n'est pas habilité à donner les renseignements ou ne peut le faire que partiellement, il transmet la demande aux autres maîtres de fichier compétents qui à leur tour informent la personne concernée.
- Lorsqu'un tiers traite des données sur mandat, le mandant est en principe tenu de donner les renseignements demandés, dans la mesure où il est lui-même maître du fichier (art. 1, al. 6). Cette obligation incombe au tiers s'il ne révèle pas l'identité du maître du fichier ou si ce dernier n'a pas de domicile en Suisse (art. 8, al. 4, LPD). Toutefois, il est des situations où le mandant ne dispose pas des renseignements demandés, le tiers étant lui-même le maître du fichier. Ce dernier n'est pas connu de la personne concernée, alors que le mandant l'est et semble être le maître du fichier. Dans ces cas, conformément au principe de la bonne foi, le mandant doit transmettre la demande d'accès au maître du fichier réel. De telles situations sont fréquentes dans le secteur de la publicité adressée: Des maisons adressent des messages publicitaires pour le compte de tiers, voire même encaissent des dons pour ces mêmes tiers, sans que la personne concernée soit informée de l'existence de cet intermédiaire. Cette disposition vise non seulement le secteur privé mais aussi les organes fédéraux (art. 10a LPD).
- L'alinéa 7 règle un cas particulier: les demandes de consultation de données concernant des personnes décédées. Cette disposition n'est pas à proprement une règle d'application de l'article 8 LPD. Elle détermine les conditions auxquelles une personne peut consulter des données relatives à une personne décédée tout en garantissant la protection de la personnalité des proches. Cette disposition reprend les principes minimaux dégagés par la jurisprudence relative à l'article 4 Constitution (voir notamment JAAC 1991 55/I 3).

3.2 Gratuité du droit d'accès et exceptions (art. 2 et 13)

L'article 8, alinéa 5, LPD prévoit que le droit d'accès est en principe gratuit. Le Conseil fédéral peut prévoir des exceptions. Ces exceptions devraient être limitées, car l'exercice d'un droit fondamental lié à la liberté personnelle ne peut raisonnablement dépendre du prélèvement d'une taxe. Deux exceptions (art. 2 et 13) lorsque:

- la personne concernée a déjà obtenu les renseignements dans les douze mois précédents. Par cette disposition, on veut éviter des demandes d'accès abusives et chicanières. Le maître du fichier ne peut toutefois pas exiger d'émolument si la personne concernée justifie d'un intérêt digne de protection en invoquant notamment le fait que les données ont entre temps été modifiées sans qu'elle en ait été informée;
- l'octroi des renseignements occasionne un volume de travail considérable. Ce motif peut notamment être invoqué lorsque les données sont traitées à des fins statistiques et qu'elles sont conservées sous une forme partiellement anonyme, lorsque l'accès nécessite de longues recherches, notamment du fait que le fichier est géré manuellement et renvoie à différents dossiers. Dans une certaine mesure, il en va de même de l'entreprise qui gère des fichiers pour ses besoins internes uniquement et qui n'est pas organisée de manière à communiquer des données ou à octroyer des renseignements. Toutefois, les maîtres de fichiers doivent veiller à organiser leurs fichiers de manière à permettre à la personne concernée d'exercer ses droits d'accès et de rectification (art. 38, al. 2, LPD). Ce motif ne peut être invoqué lorsque le volume de travail résulte d'une mauvaise organisation et gestion des fichiers du maître de fichier requis.

Le montant exigé doit cependant être raisonnable afin de ne pas être dissuasif pour la personne concernée. Il doit permettre de couvrir une partie des frais occasionnés, mais ne doit en aucun cas dépasser 300 francs. Cette limite est nécessaire, car selon la complexité du système, l'octroi du renseignement pourrait atteindre des sommes plus élevées afin de respecter le principe de la couverture des frais. Les termes de "montant équitable" désignent la redevance que l'on demande à l'intéressé et non le coût réel de l'opération. Avant qu'un tel montant ne soit prélevé, la personne concernée doit en être informée et avoir la possibilité de retirer sa demande ou de contester le montant exigé: le maître du fichier qui exige une participation doit en motiver les raisons. Lorsqu'un organe fédéral estime être en droit de prélever un émolument conformément à l'article 2, alinéa 1, la personne concernée peut exiger une décision sujette à recours conformément à l'article 25 LPD.

3.3 Droit d'accès auprès des missions suisses à l'étranger (art. 14)

L'article 14 de l'ordonnance règle les modalités d'exercice du droit d'accès auprès des représentations suisses à l'étranger et des missions auprès des organisations internationales. En effet, pour des questions de convenance diplomatique et de praticabilité, il n'est pas opportun que les demandes d'accès soient directement traitées par nos représentations à l'étranger ou nos missions auprès des organisations internationales. Il revient dès lors au Département fédéral des affaires étrangères d'examiner les demandes et le cas échéant de donner les renseignements demandés.

4. Déclaration des fichiers (*art. 3 et 4; 16, 18 OLPD)*

4.1 Dans le secteur privé (art. 3 et 4)

4.1.1 Contenu de la déclaration (art. 3)

Les fichiers qui en vertu de l'article 11a, alinéa 3 LPD doivent être annoncés au préposé, le seront avant d'être opérationnels. Il s'agit des cas où une personne privée traite régulièrement des données sensibles ou des profils de personnalité ou communique régulièrement des données personnelles à des tiers qu'ils s'agissent de données sensibles, de profils de personnalité ou d'autres données personnelles.

La déclaration du fichier donnera des informations sur:

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

Les maîtres de fichier doivent régulièrement mettre à jour les informations objets de la déclaration.

4.1.2. Exceptions à l'obligation de déclarer (art. 4)

L'article 11a, alinéa. 5 LPD introduit cependant toute une série d'exceptions à l'obligation d'annonce, notamment lorsque

- les données sont traitées en vertu d'une obligation légale
- le traitement est désigné par le Conseil fédéral comme n'étant pas susceptible de menacer les droits de la personne concernée
- le maître du fichier utilise le fichier exclusivement 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
- les données sont traitées par un journaliste qui se sert du fichier comme un instrument de travail personnel

- 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
- le maître du fichier s'est soumis à une procédure de certification au sens de l'article 11 LPD, a obtenu un label de qualité et a annoncé le résultat de la procédure de certification au préposé.

L'article 4 concrétise ainsi l'article 11a, alinéa 5, lettre b LPD selon lequel le maître du fichier n'est pas tenu de déclarer son fichier si le traitement est désigné par le Conseil fédéral comme n'étant pas susceptible de menacer les droits de la personne concernée.

L'article 4 rappelle en premier lieu que les fichiers visés au nouvel art. 11a, alinéa 5, lettres a, c à f, LPD ne sont pas soumis à déclaration, puis énumère les exceptions suivantes:

- la lettre a prévoit une exception pour les fichiers de fournisseurs ou de clients. Il s'agit par exemple de fichiers servant à la correspondance commerciale dans le cadre de l'exécution d'un contrat. Cette exception correspond à l'exception prévue à l'art. 18, alinéa 1, lettre b, OLPD pour les organes fédéraux : dans les deux cas, les fichiers de fournisseurs ou de clients ne doivent contenir ni des données sensibles ni des profils de la personnalité.
- la lettre b vise les fichiers dont les données sont traitées uniquement à des fins ne se rapportant pas aux personnes concernées, notamment dans le cadre de la recherche, de la planification ou de la statistique. Cette exception se justifie par le fait que ce type de traitement, de par sa finalité, ne porte en principe pas atteinte aux droits de la personnalité. Une telle exception est déjà prévue par le droit en vigueur en relation avec l'obligation de déclarer les communications transfrontières (art. 7, al. 1, OLPD).
- la lettre c prévoit une exception pour les fichiers qui sont archivés et dont les données ne sont conservées qu'à des fins historiques ou scientifiques. Cette exception s'inspire de l'article 18, alinéa 1, lettre b, OLPD qui prévoit que les organes fédéraux ne sont pas tenus de déclarer les fichiers qui sont conservés aux Archives fédérales.
- La lettre d concerne les fichiers contenant exclusivement des données qui ont été publiées ou qui ont été rendues accessibles au public par la personne concernée sans que cette dernière ne se soit formellement opposée au traitement.
- La lettre e vise les fichiers de journalisation. En vertu de l'article 10 OLPD, le maître du fichier journalise les traitements automatisés des données sensibles ou des profils de la personnalité lorsque des mesures préventives ne peuvent pas garantir la protection des données. Il s'agit en particulier de permettre une vérification a posteriori de l'identité des personnes introduisant des données dans un système. Le fichier des données collectées à cette fin ne doit pas être déclaré au préposé. La mesure de journalisation sert en premier lieu à protéger la personne dont les données sont traitées dans le système en question. Le risque d'abus envers des personnes qui travaillent avec le système et dont les données d'accès sont saisies est en comparaison limité.
- la lettre f prévoit une exception en faveur des pièces comptables à l'instar de l'article 18, alinéa 1, lettre e OLPD applicable au secteur public.
- l'exception de la lettre g vise les fichiers auxiliaires concernant la gestion du personnel du maître du fichier ne devront pas être déclarés, à la condition toutefois qu'ils ne contiennent ni des données sensibles ni des profils de la personnalité. Cette disposition correspond à l'exception prévue à l'article 18, alinéa. 1, lettre f OLPD.

L'article 4, alinéa 2, OLPD prévoit que le maître du fichier est tenu de prendre les mesures nécessaires afin de pouvoir communiquer au préposé et aux personnes concernées qui en font la demande les informations énumérées à l'article 3, alinéa 1 OLPD. Cette obligation découle des articles 8 et 29, alinéa 2 LPD.

4.2 Dans le secteur public (art. 16 et 18 OLPD)

4.2.1 Déclaration

Conformément à l'article 11a LPD, les organes fédéraux sont tenus de déclarer tous leurs fichiers avant qu'ils ne soient opérationnels. Cette obligation est énoncée à l'article 16 de l'ordonnance. L'annonce contiendra les mêmes informations que dans le secteur privé, avec en plus l'indication de la base légale. Les organes fédéraux sont tenus de mettre à jour ces informations.

4.2.2 Exceptions à l'obligation de déclarer

Avec la révision de la LPD et de l'OLPD, le système de la déclaration simplifiée de certaines catégories de fichiers a été abandonné. Il en va de même des exceptions à la publication. Ces fichiers font désormais partie des exceptions à la déclaration. A l'instar de l'article 4 OLPD, l'article 18 énonce les fichiers de données personnelles dont le traitement n'est pas susceptible de menacer les droits de la personne concernée:

l'article 18, alinéa 1, lettre a vise les fichiers usuels d'enregistrement de la correspondance. Par fichier usuel d'enregistrement de la correspondance, il faut entendre un fichier simple qui répertorie le courrier et contient notamment le nom et l'adresse du demandeur, la date d'entrée, le collaborateur responsable de la demande, la réponse et la date de sortie (répertoire de correspondance). L'accès au fichier est en soi limité à un cercle restreint d'utilisateurs, en particulier les personnes responsables de l'enregistrement de la correspondance. Un fichier recensant les lettres des citoyens peut entrer dans cette catégorie. Par contre si le système permet différentes opérations qui dépassent le simple répertoire de correspondance ou contient d'autres données et notamment des données sensibles ou des profils de la personnalité, provenant du traitement de la demande et impliquant des opérations plus complexes qui nécessitent la collecte et l'enregistrement dans le système de données provenant de tiers, d'expertises, d'éclaircissements, de procès-verbaux d'enquête ou d'audition, etc., nous ne sommes plus en présence d'un simple fichier d'enregistrement de la correspondance, mais d'un système de gestion et de documentation. Les systèmes GEVER ne sont ainsi en principe pas des fichiers usuels d'enregistrement de la correspondance et doivent être annoncés. Il s'agit de systèmes complexes de traitement des données qui intègrent différentes fonctionnalités et qui peuvent contenir des données sensibles et des profils de la personnalité. Au sein d'un département ou d'un office, ces systèmes peuvent être accessibles à différents services ou entités et offrir de nombreux accès qui ne sont pas uniquement réservés à un seul service ou un seul office.

- L'article 18, alinéa 1, lettre b concerne les fichiers de fournisseurs ou de clients, dans la mesure où ils ne contiennent pas de données sensibles ou de profils de la personnalité.
- L'article 18, alinéa 1, lettre c vise les fichiers d'adresses qui servent uniquement à l'envoi de correspondance, dans la mesure où ils ne contiennent pas de données sensibles ou de profils de la personnalité (liste de commissions d'experts, par ex.; cela même si ces listes sont distribuées à des tiers).
- L'article 18, alinéa 1, lettres d et e concernent les listes qui servent au paiement des indemnités, et les pièces comptables.
- L'article 18, alinéa 1, lettre f prévoit que les fichiers auxiliaires concernant la gestion du personnel de la Confédération ne doivent pas être déclarés lorsqu'ils ne contiennent pas de données sensibles ou de profils de la personnalité.
- L'article 18, alinéa 1, lettre g vise les fichiers des bibliothèques (catalogues, listes de prêts et d'utilisateurs).
- L'article 18, alinéa 2, lettre a concerne les fichiers qui sont déposés aux Archives fédérales.
- L'article 18, alinéa 2, lettre b vise les fichiers qui sont rendus accessibles au public sous forme d'annuaires.
- L'article 18, alinéa 2, lettre c introduit une exception pour les fichiers dont les données sont traitées uniquement à des fins ne se rapportant pas aux personnes concernées, notamment dans le cadre de la statistique, de la recherche ou de la planification.

- L'article 18, alinéa 3 prévoit que l'organe fédéral responsable prend les mesures nécessaires afin de pouvoir communiquer au préposé ou aux personnes concernées qui en font la demande les informations y relatives (art. 16, al. 1, OLPD). Cette obligation découle des articles 8 et 27 LPD.

5. Communication des données à l'étranger (art. 5 à 7, 19 OLPD)

5.1 Publication sous forme électronique (art. 5)

La teneur de l'ancien article 5 OLPD n'a pas été maintenue. En effet, les définitions de cette disposition ne sont plus appropriées, vu que le nouvel article 6 LPD ne vise plus seulement la communication de fichiers mais aussi la communication de données personnelles. Cette modification n'a toutefois pas de conséquence matérielle. L'accès à des données personnelles par procédure d'appel et la transmission d'un fichier à un tiers pour effectuer un traitement pour le compte de celui qui transmet le fichier constituent, comme aujourd'hui, une communication transfrontière de données.

L'article 5 OLPD introduit une nouvelle disposition concernant la publication de données personnelles par Internet ou par un autre service d'information ou de communication aux fins d'information du public. Il est possible de consulter sur Internet des informations contenant ou non des données personnelles à l'étranger, y compris dans un Etat qui n'est pas en mesure de garantir une protection adéquate des données personnelles. Ces données peuvent également être traitées dans le pays en question. La publication de données personnelles sur Internet ne vise donc pas forcément une communication à l'étranger. Une telle communication n'est en fait qu'une conséquence de la publication sur internet. L'article 5 qui s'appuie sur l'article 19, al. 3bis LPD, tient compte de ce mécanisme[1].

5.2 Devoir d'information (art. 6)

L'obligation de déclarer les communications de données à l'étranger a été remplacée par une obligation d'informer le préposé. L'article 6, alinéa 3, LPD prévoit que le préposé doit être informé des garanties et des règles de protection des données visées à l'article 6, alinéa 2, lettres a et g, et que le Conseil fédéral règle les modalités du devoir d'information. Selon le message (FF 2003, p. 1942), l'ordonnance d'exécution doit préciser à quel moment cette information doit être donnée et de quelle manière.

L'article 6, alinéa. 1, OLPD prévoit que le maître du fichier informe le préposé, avant la communication à l'étranger. Cette disposition ne fixe donc pas un délai précis mais laisse une certaine flexibilité au maître du fichier. Si ce dernier n'est pas en mesure d'informer le préposé avant la communication des données, il remédie à cette situation dans les meilleurs délais. Cette information consiste à transmettre au préposé un exemplaire ou une copie des garanties convenues avec le destinataire ou des règles de protection des données applicables au sein de la société ou des sociétés concernées. Comme il résulte du message (FF 2003, p. 1942), la procédure d'information doit être aussi simple que possible ; le préposé peut par exemple être informé par courriel.

Comme il résulte du message (FF 2003, p. 1942), le devoir d'information prévu à l'article 6, alinéa 3, LPD ne signifie pas que le maître du fichier a l'obligation d'informer le préposé de chaque communication particulière. L'article 6, alinéa 2 précise ce point. Selon la lettre a, une fois les garanties annoncées au préposé, le devoir d'information du maître du fichier est réputé également rempli pour toutes les communications qui se basent sur les mêmes garanties, pour autant que les catégories de destinataires, les finalités de traitement et les catégories de données restent similaires. Cette disposition offre donc une certaine flexibilité au maître du fichier.

Quant aux règles de protection des données établies au sein d'une même personne morale ou société ou entre des personnes morales ou sociétés réunies sous une direction unique, elles s'appliquent à toutes les communications de données effectuées entre elles, indépendamment de la catégorie des données communiquées et de la finalité poursuivie. Le devoir d'information vaut donc de manière

---

[1] Voir à ce sujet le jugement de la Cour de justice des Communautés européennes du 6 novembre 2003 dans la cause C-101/01 Lindqvist, ch. 56ss.

globale pour toutes ces communications, aussi longtemps que les règles fournies permettent de garantir une protection adéquate des données (art. 6, al. 2, let. b). Des modifications ou des adaptations sont donc possibles dans une certaine mesure, sans que le préposé doive en être à nouveau informé.

L'article 6, alinéa 3 prévoit un devoir d'information allégé, lorsque le maître du fichier utilise les contrats modèles ou des clauses standards établis ou reconnus par le préposé, tels que les clauses modèles du contrat type du Conseil de l'Europe. Le maître du fichier doit uniquement informer le préposé qu'il utilise les contrats modèles ou les clauses standards reconnus par ce dernier pour communiquer des données vers un Etat qui ne dispose pas d'une législation assurant un niveau de protection adéquat. Il s'ensuit que le maître du fichier n'est plus tenu d'informer le préposé sur chaque communication ou catégorie de communications. Cependant, s'il utilise d'autres garanties pour des cas déterminés, le devoir d'informer le préposé s'applique.

Cette disposition s'applique également aux organes fédéraux lorsqu'ils communiquent des données sur la base de l'article 6, alinéa 2, lettre a LPD (art. 19 OLPD).

La 2ème phrase de l'alinéa 3 charge le préposé de publier une liste des contrats modèles ou des clauses standards qui peuvent être utilisés.

Selon le message (FF 2003, p. 1941), le maître du fichier qui communique des données à l'étranger est responsable du préjudice qui pourrait résulter d'une violation de l'obligation de diligence. Il lui incombe en particulier de démontrer qu'il a pris toutes les mesures nécessaires pour s'assurer d'un niveau de protection adéquat. L'ordonnance met en oeuvre cette obligation de diligence en prévoyant que le maître du fichier prend les mesures adéquates pour s'assurer que le destinataire respecte les garanties ou les règles de protection des données (al. 4). La question de savoir si les mesures sont adéquates dépend des circonstances du cas d'espèce. Les exigences seront plus élevées s'il s'agit de données sensibles ou de profils de la personnalité que pour les autres données personnelles. En cas de non-respect des garanties ou des règles de protection par le destinataire, le maître du fichier l'invite à remédier à cette situation.

L'alinéa 5 fixe un délai de 30 jours au préposé pour examiner si les garanties ou les règles de protection qui lui sont annoncées assurent un niveau de protection adéquat au sens des exigences de la Convention STE 108. Si tel n'est pas le cas, il intervient auprès du maître du fichier et émet, le cas échéant, une recommandation conformément à l'article 29 LPD. A défaut de réaction de la part du préposé dans le délai fixé, le maître du fichier peut partir de l'idée que le préposé n'a pas d'objection contre les garanties et les règles de protection des données fournies.

5.3 Liste des Etats disposant d'une législation assurant un niveau de protection adéquat (art. 7)

L'article 7 OLPD prévoit que le préposé publie une liste des Etats ayant adopté une législation assurant un niveau de protection adéquat. Pour établir cette liste, le préposé doit tenir compte des décisions d'adéquation de la Commission européenne prises en application de l'article 25, § 6, de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Si le maître du fichier communique des données à destination d'un Etat mentionné dans la liste du préposé, il est présumé de bonne foi au sens de l'article 3, alinéa 1, CC. Il s'agit toutefois d'une présomption réfragable. En effet, en vertu de l'alinéa 2, le maître du fichier ne peut invoquer sa bonne foi, par exemple, s'il a pu constater sur la base de son expérience que les prescriptions de protection des données ne sont pas respectées dans un pays déterminé.

6. Mesures techniques et organisationnelles (art. 8 à 12, 20 à 22 OLPD)

6.1 Dans le secteur privé (art. 8 à 12)

6.1.1 Principe et objet (art. 8)

Parmi les principes fondamentaux régissant le traitement des données personnelles figure le principe de la sécurité des données (art. 7 LPD). Aux termes de cette disposition, quiconque traite des données personnelles doit prendre des mesures organisationnelles et techniques appropriées pour protéger ces données contre tout traitement non autorisé. Il revient au Conseil fédéral d'édicter des dispositions plus détaillées et en particulier de fixer les exigences minimales en matière de sécurité des données. La sécurité des données est une exigence fondamentale dans l'édifice de la protection des données. Elle concerne la protection des informations, alors que la protection des données vise la protection des personnes. Elle permet d'assurer la confidentialité, la disponibilité et l'intégrité des données afin de garantir de manière appropriée la protection des données. Les mesures à prendre pour garantir la sécurité des données sont d'ordre technique et organisationnel. La sécurité absolue n'existe pas. En outre, elle doit être différenciée en fonction des finalités du traitement, de la nature des données traitées, de l'étendue du traitement et des risques encourus par les personnes concernées (principe de proportionnalité, art. 8, al. 2). Elle doit tenir compte de l'état du développement de la technique et dans une moindre mesure des coûts et de la capacité financière de l'entreprise. L'ordonnance (art. 8 à 12) définit le cadre minimum à atteindre en matière de sécurité des données en faisant application du principe de proportionnalité par la mise en balance des différents intérêts en présence. Sous réserve de l'article 10 qui introduit une obligation de journaliser certains traitements portant sur des données sensibles ou des profils de la personnalité, l'ordonnance ne prescrit aucune mesure technique particulière, tel que mot de passe, autres mesures techniques d'identification, chiffrement des données, etc. Il revient au maître du fichier d'apprécier selon les critères susmentionnés. L'ordonnance tient compte du fait que la sécurité des données est un processus évolutif lié au développement de la technique, processus qui nécessite une réévaluation périodique (art. 8, al. 3).

L'article 8, alinéa 1 énumère les risques contre lesquels il y a lieu de protéger les données dans la mesure où cela est nécessaire et propre à garantir la protection des données, c.à.d. la protection de la personnalité des personnes. Il s'agit en particulier des risques suivants:

- destruction accidentelle ou non autorisée;
- perte accidentelle;
- erreurs techniques;
- falsification, vol ou utilisation illicite;
- modification, copie, accès ou autres traitements non autorisés.

6.1.2 Traitements et fichiers automatisés (art. 9)

La finalité des mesures techniques et organisationnelles, notamment en présence de fichiers automatisés ou de systèmes d'informations automatisés est d'éviter que ces fichiers ou ces systèmes ne permettent plus que ce qu'ils ne doivent. A cet effet, l'ordonnance (art. 9, al. 1) énonce une série d'objectifs à atteindre en particulier lors de traitements automatisés. A dessein, ces mesures ne se limitent pas à l'existence d'un fichier, puisque la tendance actuelle va vers une plus grande dispersion des informations dans de vastes systèmes d'informations répondant à des schémas d'organisation différents mais qui permettent néanmoins un usage par personne concernée. Par rapport à ces nouvelles tendances informatiques et télématiques, la notion de fichier est dépassée. Par ce choix, l'OLPD suit également l'évolution des législations européennes récentes et en particulier le projet de directive des Communautés européennes.

Les objectifs énoncés à l'article 9, alinéa 1 sont au nombre de huit. Ils doivent être réalisés conformément au principe de proportionnalité et tenir compte, comme pour l'ensemble des autres mesures de sécurité, des finalités, de la nature et de l'étendue du traitement, de l'évaluation des risques potentiels pour les personnes concernées et du développement actuel. Un système d'informations en matière de protection de l'Etat ou un fichier de santé ne *répondra* pas aux mêmes niveaux de sécurité qu'un fichier d'adresses.

Il s'agit des huit objectifs suivants:

- contrôle à l'entrée des installations: il s'agit ici de prendre des mesures propres à éviter que des personnes non autorisées aient accès aux installations utilisées pour le traitement de données personnelles, notamment l'accès aux locaux où sont situés les ordinateurs. Cet

objectif ne vise pas uniquement l'accès à un ordinateur central, mais également les périphériques, tels que les terminaux.

- contrôle des supports de données: ce contrôle doit permettre d'éviter qu'une personne non autorisée puisse lire, copier, modifier ou éloigner des supports de données. En particulier, il faut veiller à empêcher que des données puissent être déchargées de manière incontrôlée sur des supports de données. Un support de données est un support physique sur lequel des données peuvent être transcrites (papier, image, carte perforée, support magnétique, disque dur, disquette, bande, disque compact, carte/support optique, etc.). N'est considéré comme support de données que le support indépendant c.à.d. qui n'est pas intégré au fichier, à l'ordinateur, au système informatique ou à l'installation principale de conservation des données.
- contrôle de transport: cet objectif tend à éviter qu'une personne non autorisée puisse prendre connaissance des données (copier, modifier, effacer) lors de leur communication. Le destinataire des informations doit également avoir l'assurance que les données qu'il reçoit sont bien celles qui lui ont été envoyées et qu'aucun tiers ne les a interceptées de manière illicite. Ainsi, en cas de risque particulièrement élevé d'atteinte à la vie privée et aux droits des personnes concernées, notamment du fait que des données sensibles ou des profils de la personnalité sont communiqués, on recourra à des méthodes de chiffrement des données ou à des mesures offrant une sécurité équivalente.
- contrôle de communication: cette mesure doit permettre d'identifier les destinataires des données, c'est-à-dire vérifier et constater à quelles personnes ou organes des données sont communiquées. Elle doit permettre de contrôler au besoin au moyen de quelle installation et à qui les données ont été communiquées, notamment en journalisant les communications. La journalisation ne doit pas toujours être introduite, mais il faut être en mesure d'examiner le déroulement des opérations.
- contrôle de mémoire: cet objectif tend à empêcher qu'une personne non autorisée puisse avoir accès à un fichier ou à un système de traitement automatisé, et en particulier prendre connaissance du contenu de la mémoire (unité fonctionnelle qui peut recevoir, conserver et restituer des données), le modifier ou l'effacer. Il faut ainsi introduire des mesures afin que seules les personnes autorisées puissent utiliser les données enregistrées dans le fichier ou le système de traitement automatisé et ce dans les limites de leur autorisation.
- contrôle d'utilisation: par cet objectif, on veut éviter qu'une personne non autorisée ne puisse utiliser un système de traitement automatisé, notamment en recourant à des installations de communication des données. Il s'agit en particulier d'empêcher des tiers de pénétrer dans le système.
- contrôle d'accès: par cet objectif, il faut garantir que seules les personnes autorisées ont accès aux seules données dont elles ont besoin pour l'accomplissement de leurs tâches. Ainsi, le maître du fichier doit délivrer des autorisations d'accès différenciées en fonction des tâches que chaque utilisateur est appelé à exécuter. Ces autorisations d'accès donnent le droit de traiter des données dans une mesure préalablement déterminée et pour une finalité prédéfinie. Elles doivent en particulier décrire la nature et l'étendue des accès.
- contrôle de l'introduction: cet objectif tend à assurer qu'un contrôle a posteriori des données introduites dans le fichier ou le système soit possible. Ce contrôle doit porter également sur la personne qui procède à l'introduction des données et sur le moment où l'opération a été effectuée. Il s'agit ici de permettre un suivi de l'introduction des données. Ce suivi ne nécessite pas obligatoirement une journalisation. L'introduction doit cependant pouvoir être contrôlée à l'aide des documents à disposition.

L'article 9, alinéa 2 énonce une règle relative à l'organisation des fichiers. Ceux-ci doivent être organisés de manière à permettre aux personnes concernées d'exercer leur droit d'accès. Cela implique en particulier que des mesures techniques et organisationnelles soient prises pour leur délivrer le contenu des données les concernant.

6.1.3 Journalisation (art. 10)

L'article 10 de l'ordonnance prévoit en outre une obligation de journaliser les traitements automatisés de données sensibles ou de profils de la personnalité afin de permettre une vérification a posteriori. Cette journalisation ne doit intervenir que dans la mesure où le maître de fichier n'a pas pris d'autres mesures préventives permettant de garantir la protection des données et d'assurer que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées. A titre d'exemples de mesures préventives, on peut citer la séparation fonctionnelle entre les données personnelles et les programmes, les accès différenciés en fonction des utilisateurs et des tâches à accomplir, les codes d'accès, le principe des 4 yeux, etc. Le préposé fédéral peut recommander la journalisation pour d'autres traitements lorsqu'ils présentent un risque élevé d'atteinte à la vie privée et aux droits des personnes concernées. Ce peut être le cas de fichiers ou de traitements qui sans contenir des données sensibles au sens de l'article 3, lettre c, LPD présentent un certain degré de sensibilité notamment du fait du domaine dans lequel ils sont gérés (assurances, agence de renseignements, etc.) et de la configuration du système d'informations, en particulier lors de l'accès aux données par procédure d'appel.

Cette vérification doit permettre avant tout de contrôler que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées. Il s'agit en particulier de contrôler que les données ne sont pas utilisées à des fins non prévues ou non compatibles. Un tel risque est d'autant plus élevé que les données sont enregistrées dans un système d'information accessible à un nombre élevé d'utilisateurs ou connectés physiquement ou optiquement à d'autres fichiers. Il n'est pas nécessaire de tout journaliser. Il faut ici également tenir compte du principe énoncé à l'article 8 et faire application du principe de proportionnalité (art. 4, al. 2 LPD et 8, al. 2 OLPD). Les procès-verbaux de journalisation servent à contrôler que les dispositions de protection des données ont été respectées. Ils ne doivent dès lors être rendus accessibles qu'aux seuls organes ou personnes chargés de vérifier l'application de ces dispositions, notamment le préposé fédéral et les organes internes de contrôle (responsables de la protection et de la sécurité des données dans l'entreprise ou dans une unité administrative). Ces procès-verbaux doivent être conservés durant une année sous une forme permettant d'effectuer le contrôle, c'est-à-dire qu'ils ne doivent en particulier pas pouvoir être modifiés.

6.1.4 Règlement de traitement (art. 11)

Parmi les mesures techniques et organisationnelles, l'article 11 prévoit l'obligation d'élaborer un règlement de traitement pour les fichiers automatisés du secteur privé soumis à déclaration conformément à l'article 11a, alinéa 3, LPD. Il en découle que le maître du fichier qui traite des données sensibles ou des profils de la personnalité ou qui communique régulièrement des données personnelles à des tiers, est en principe tenu de déclarer ses fichiers et d'élaborer un règlement. Il sera toutefois délié de son obligation d'élaborer un règlement si son fichier tombe sous le coup d'une des exceptions prévues à l'article 11a, alinéa 5, lettre b à d, LPD. En revanche s'il désigne un conseiller à la protection des données (art. 11a, al. 5, let. e, LPD) ou s'il souhaite obtenir un label de qualité en matière de protection des données, il devra élaborer un règlement même s'il est délié de son obligation de déclaration. Il en va de même lorsque des données sont traitées en vertu d'une obligation légale (art. 11a, al. 5, let. a, LPD).

Le règlement de traitement doit être conçu comme une documentation ou un manuel géré par le maître de fichier. Ce règlement donne des informations sur l'organisation interne du maître du fichier, sur l'organisation et la structure dans laquelle se situe le fichier ou le système de traitement automatisé. Il décrit en particulier les procédures de traitement et de contrôle des données. Il comprend des documents relatifs à l'élaboration, à la planification et à la gestion du fichier et des moyens informatiques mis en œuvre. Ce règlement doit être régulièrement mis à jour et tenu à disposition du préposé ou du conseiller à la protection des données au sens de l'article 11a, alinéa 5, lettre e LPD sous une forme qui leur soit intelligible.

6.1.5 Communication de données (art. 12)

L'article 12 prévoit qu'avant la communication des données, le destinataire des données soit renseigné sur l'actualité et la fiabilité des données. Ainsi, dans la mesure où cela ne ressort pas des

circonstances ou des données elles-mêmes, la personne privée qui communique indiquera en particulier la date de la dernière mise à jour et précisera si les données sont sûres ou incertaines quant à leur exactitude. Cette exigence découle directement du principe de l'exactitude des données énoncé à l'article 5 LPD. Elle est également dans l'intérêt de la personne qui communique, laquelle engage sa responsabilité si elle communique des données fausses.

6.2 Dans le secteur public (art. 20 à 22)

6.2.1 Mesures techniques et organisationnelles: principes (art. 20)

L'article 20 prévoit que les organes fédéraux responsables du traitement et du fichier au sens de l'article 16 LPD prennent des mesures techniques et organisationnelles propres à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données. Ces mesures sont identiques à celles prescrites pour le secteur privé (art. 8 à 10, voir commentaire sous points 6.1.1, 6.1.2 et 6.1.3 ci-dessus). En présence de traitement automatisé, les organes responsables collaborent avec l'Unité de stratégie informatique de la Confédération (USIC). L'ordonnance du 26 septembre 2003 sur l'informatique dans l'administration fédérale (OIAF, RS 172.010.58) demeure applicable (art. 20, 4e al.).

Non seulement pour des raisons financières et d'efficacité, mais également pour tenir compte des exigences de la protection des données, il est nécessaire d' intégrer lesdites exigences dès les premières phases de développement d'un projet informatique. Ainsi, l'article 20 OLPD prévoit une obligation pour les organes fédéraux de soumettre à leur conseiller à la protection des données au sens de l'article 11a LPD tous leurs projets de traitement automatisé de données personnelles dès le début de leur développement (art. 20, al. 2, OLPD). A défaut d'un tel conseiller, le projet doit être transmis au préposé. L'annonce au préposé se fait par l'entremise de l'USIC lorsque les projets doivent également lui être annoncés. Pour les autres projets, l'annonce se fait directement au préposé fédéral.

Afin d'éviter des doubles emplois et des actions en ordre dispersé, l'article 20, alinéa 3, prévoit une collaboration entre le préposé et l'USIC dans l'examen et le contrôle des mesures techniques nécessaires à garantir la protection des données. En particulier, le préposé prend l'avis *de l'USIC* avant d'émettre une recommandation.

6.2.2 Règlement de traitement (art. 21)

Parmi les mesures techniques et organisationnelles, l'article 21 prévoit l'adoption de règlements de traitement pour les fichiers fédéraux automatisés qui contiennent des données sensibles, qui sont utilisés par plusieurs organes fédéraux (tel par exemple le système *BV+*) ou qui sont rendus accessibles aux cantons (tel par exemple les systèmes RIPOL, ZEMIS), à des autorités étrangères, à des organisations internationales ou à des personnes privées. Le règlement de traitement doit être conçu comme une documentation gérée par l'organe responsable qui donne des informations sur son organisation interne et celle des organes ou personnes participant au fichier. Le règlement donne des informations sur l'organisation et la structure dans laquelle se situe le fichier ou le système de traitement automatisé, ainsi que des informations sur l'accomplissement par les utilisateurs de leurs tâches dans le temps et dans l'espace. Il doit en particulier décrire les procédures de traitements des données, les procédures de contrôle, le déroulement des principales opérations de traitement. Le règlement documente sur l'élaboration et la gestion du fichier (présentation des diverses fonctions du système ou du fichier, périodicité des traitements).

Un tel règlement est dans l'intérêt de tout responsable d'un traitement automatisé, non seulement dans l'optique de la protection des données, mais également dans celle d'une exploitation rationnelle. Il doit également servir de manuel de l'utilisateur et être mis à disposition des organes chargés du contrôle. Pour être utile, il est nécessaire qu'il soit constamment mis à jour. Un tel règlement ne constitue pas en soi une charge de travail supplémentaire pour l'organe responsable. Il s'agit en fait de mettre sous un même toit des règles et des informations qu'il doit sans autres détenir. Un tel règlement doit tout d'abord contenir les informations nécessaires à l'annonce du fichier conformément à l'article 16 OLPD. Ces informations doivent être complétées par des informations sur la source des données (on pourra également y indiquer la procédure de collecte des données et la manière de les

saisir), sur les finalités pour lesquelles les données sont régulièrement communiquées ou échangées, sur les procédures de contrôle et plus précisément sur les mesures techniques et organisationnelles, y compris la réglementation des accès des différents utilisateurs, la description des champs de données et leur rattachement aux différentes unités d'organisation et d'exécution (en particulier les accès des utilisateurs, la nature et l'étendue de ces accès par rapport aux tâches à accomplir), les procédures de traitement des données et notamment la procédure à suivre lorsque la personne concernée fait usage de son droit d'interdire une communication ou un traitement de données, la durée de conservation des données personnelles et la procédure d'anonymisation, d'archivage ou de destruction des données, ainsi que sur la configuration des moyens informatiques utilisés pour l'accomplissement des tâches (informations techniques sur les installations, notamment emplacement des terminaux, description des supports de données et du mode de communication des données, les réseaux, ainsi que les matériels et les logiciels utilisés). Enfin, le règlement doit préciser la procédure d'exercice du droit d'accès des personnes concernées et indiquer l'organe ou la personne responsable de la protection et de la sécurité des données.

6.2.3 Traitement de données sur mandat (art. 22)

La LPD règle expressément le traitement sur mandat effectué ou confié par des organes fédéraux à l'article 10a LPD. L'article 36, 4e alinéa, lettre b, LPD confère au Conseil fédéral la compétence de préciser les conditions d'un tel traitement. Ainsi aux termes de l'article 22 OLPD, lors du traitement par un tiers, l'organe fédéral qui fait traiter des données personnelles demeure responsable de la protection des données. Cela implique pour lui l'obligation de veiller à ce que le traitement s'effectue conformément au mandat et que le mandataire ne traite les données que pour l'exécution du mandat. Il doit également assurer l'exercice du droit d'accès. En règle générale, l'octroi d'un mandat devrait faire l'objet d'un contrat écrit entre l'organe fédéral et le tiers mandaté lorsque celui-ci n'est pas lui-même un organe fédéral. Un tel contrat devra en tous les cas être conclu lorsque le mandataire n'est pas soumis à la LPD ou à des dispositions légales offrant une protection équivalente. Entre organes fédéraux, l'octroi de mandat devrait faire l'objet d'un document écrit.

7. Conseillers à la protection des données (art. 12a et 12b, art. 23)

7.1 Secteur privé (art. 12a et 12b)

7.1.1 Désignation du conseiller (art. 12a)

L'article 11a, alinéa 5, lettre e, LPD prévoit que le maître du fichier n'est pas tenu de déclarer son fichier s'il 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. Selon le message (FF 2003, p. 1949), le Conseil fédéral peut en particulier prévoir que le maître du fichier n'est délié de son devoir de déclaration que s'il a annoncé au préposé la nomination d'un conseiller à la protection des données.

Les désignations, dans les versions allemande et italienne, de «Datenschutzverantwortlicher» et de «responsabile della protezione dei dati» (art. 11a, al. 5, let. e, LPD) ne signifient pas que cette personne est seule responsable du respect de la protection des données. Son activité se limite à des tâches de conseil et de surveillance. La responsabilité incombe en fait en premier lieu à l'organisme considéré comme le maître du fichier et, partant, comme le responsable de tous les traitements de données effectués. La version française de l'art. 11a, alinéa 5, lettre e, LPD est donc plus exacte («conseiller à la protection des données»).

Pour mettre en oeuvre l'art. 11a, alinéa 5, lettre e, LPD, l'article 12a, alinéa 1 OLPD prévoit que pour être délié de son devoir de déclaration, le maître du fichier doit désigner un conseiller à la protection des données qui remplit les conditions des articles 12a, alinéa 2 et 12b de l'ordonnance et en informer le préposé.

Conformément à l'alinéa 2, le maître du fichier peut désigner, en qualité de conseiller à la protection des données, un membre de son personnel. En principe, peu importe son rang hiérarchique. Toutefois, afin de garantir son indépendance, il serait opportun que la personne désignée soit directement subordonnée à l'organe de direction du maître du fichier. Le conseiller à la protection des données

peut également être un tiers. Cette solution permet de mieux garantir le principe d'indépendance exigé par la LPD et permet à des petites et moyennes entreprises de mandater un conseiller externe, sans avoir à créer une poste spécifique.

Le conseiller à la protection des données doit être indépendant dans l'exercice de ses fonctions (art. 11a, al. 5, let. e, LPD). Ce principe est concrétisé à l'article 12a, alinéa 2, 2ème phrase. En vertu de cette disposition, le maître du fichier doit désigner une personne qui n'exerce pas d'activités incompatibles avec ses tâches de conseiller à la protection des données. Il y a par exemple incompatibilité si le conseiller à la protection des données est membre de la direction, exerce des fonctions dans les domaines ayant trait à la gestion des ressources humaines, à l'administration des systèmes d'information, aux technologies de l'information ou fait partie d'un service mettant en oeuvre des traitements de données sensibles. En revanche, le cumul du poste de conseiller à la protection des données et de chargé de la sécurité informatique ou de la direction du service juridique n'est en principe pas incompatible. Le principe d'indépendance ne doit pas seulement être respecté par le maître du fichier mais aussi par le conseiller à la protection des données. En effet, l'alinéa 2 oblige ce dernier de renoncer à toute activité susceptible d'entrer en conflit avec les tâches qu'il accomplit pour le compte du maître du fichier.

Pour exercer ses tâches de manière efficace, le conseiller à la protection des données doit en outre avoir les connaissances professionnelles nécessaires (al. 2, 2ème phrase). Ses compétences doivent porter non seulement sur la législation en matière de protection des données, mais aussi sur les normes techniques, l'organisation du maître du fichier et les traitements effectués par ce dernier.

Le conseiller à la protection des données est principalement une fonction. Cette dernière peut donc être attribuée non seulement à une personne mais aussi à une équipe composée par exemple d'un spécialiste de la protection des données et d'un spécialiste en matière de sécurité informatique. Une telle solution permettrait par exemple de respecter les exigences concernant les connaissances professionnelles. Si la tâche de conseiller à la protection des données est conférée à plusieurs personnes, la responsabilité de l'exécution des tâches doit être clairement définie.

L'article 12a laisse la faculté au maître du fichier de décider s'il entend se prévaloir de l'exception prévue à l'article 11a, alinéa 5, lettre e, LPD. Si tel est le cas, il est tenu d'informer le préposé qu'il a désigné un conseiller à la protection des données. L'ordonnance ne prévoit pas d'obligation de communiquer au préposé l'identité de la personne désignée. Une telle information serait toutefois souhaitable, ne serait-ce que pour faciliter les contacts. La procédure pour informer le préposé doit être aussi simple que possible ; il peut par exemple être informé par Internet. Cette information détermine le point de départ de l'exonération du maître du fichier de l'obligation de déclarer ses fichiers. En revanche, si le conseiller à la protection des données désigné ne remplit pas les exigences d'indépendance prévues par la LPD ou si le maître du fichier renonce à se prévaloir de l'exception prévue à l'article. 11a, alinéa 5, lettre e, LPD, ce dernier reste soumis à l'obligation de déclaration et notamment devra annoncer ces fichiers du personnel lorsqu'ils contiennent des données sensibles ou des profils de la personnalité.

7.1.2 Tâches et statut (art. 12b)

Selon l'article 11a, alinéa 6, 2ème phrase, LPD, le Conseil fédéral précise le rôle et les tâches du conseiller à la protection des données. Pour mettre en oeuvre cette disposition, l'article 12b, alinéa 1 OLPD règle les tâches qui lui incombent.

- En vertu de la lettre a, le conseiller à la protection des données doit contrôler les traitements des données personnelles et proposer des corrections s'il apparaît que des prescriptions sur la protection des données ont été violées. Le maître du fichier ne doit pas sanctionner le conseiller à la protection des données du fait de l'accomplissement de sa tâche. La tâche prévue à la lettre a n'engage pas la responsabilité du conseiller à la protection des données. En effet, en cas de violation de la législation sur la protection des données, seul le maître du fichier en répond, notamment à l'égard de la personne concernée.
- Conformément à la lettre b, le conseiller à la protection des données doit dresser un inventaire des fichiers du maître du fichier. Seuls les fichiers mentionnés à l'article 11a, alinéa 3, LPD doivent y figurer. L'inventaire peut être consulté par le préposé ou par les personnes concer-

nées qui en font la demande. Il permet ainsi de garantir la transparence des fichiers qui ne sont plus soumis à déclaration, tant à l'égard des personnes concernées que du préposé.

- Même si l'ordonnance ne le prévoit pas expressément, le conseiller à la protection des données devra prendre les mesures nécessaires pour l'accomplissement de se tâches. Il devra notamment conseiller et former le maître du fichier et son personnel en édictant par exemple des directives ou des instructions. Il donnera son avis sur tous les projets qui touchent la protection des données, ce qui implique qu'il doit être consulté par le maître du fichier avant la mise en oeuvre de tout nouveau traitement. Il fera également régulièrement rapport au maître du fichier sur son activité.
- L'article 12b, alinéa 2, OLPD met en oeuvre le principe d'indépendance du conseiller à la protection des données (art. 11a, al. 5, let. e, LPD). Selon le message (FF 2003, p. 1049), il n'est pas soumis aux instructions du maître du fichier et ne doit pas lui être subordonné.
- Selon la lettre a, le conseiller à la protection des données ne reçoit pas d'instructions concernant l'exercice de sa fonction. En vertu de cette disposition, le maître du fichier doit donc s'abstenir d'intervenir auprès du conseiller à la protection des données dans le cadre de l'exécution des tâches qui lui sont attribuées. La garantie de son indépendance est essentielle. Il peut en effet se trouver dans des situations conflictuelles. Il peut par exemple être amené à juger de la licéité de traitements de données concernant le personnel du maître du fichier et à devoir préconiser des solutions organisationnelles ou techniques qui pourraient ne pas recueillir immédiatement l'assentiment de la direction ou des services concernés.
- Pour exercer ses tâches de manière indépendante, le conseiller à la protection des données doit également disposer des ressources nécessaires, notamment en ce qui concerne les moyens humains, l'infrastructure et autres équipements indispensables (let. b).
- Le conseiller à la protection des données doit avoir accès aux fichiers et aux traitements ainsi qu'à toute information nécessaire à l'accomplissement de sa tâche (let. c). Il doit également avoir la faculté d'interroger le maître du fichier et son personnel.
- Il convient enfin de relever que ni la loi ni l'ordonnance ne confèrent au conseiller à la protection des données le droit de porter l'affaire devant le préposé si ses recommandations ne sont pas suivies. Il peut par contre dans l'exercice de ces tâches demander conseil au préposé, conformément à l'article 28 LPD.

7.2 Organes fédéraux (art. 23)

L'effectivité de la protection des données exige d'une part la mise en place de garanties légales des droits de la personne concernée et d'autre part la possibilité de contrôler le respect de ces garanties. Ce contrôle se situe à plusieurs niveaux et nécessite en particulier une autorité indépendante: c'est le rôle du préposé fédéral. Toutefois, il convient également de souligner que l'organe qui traite des données personnelles est le premier responsable du respect des dispositions de protection des données (art. 16, al. 1 LPD). Dans cette optique, il convient de renforcer la structure de contrôle. Il faut rapprocher la surveillance des organes chargés du traitement des données, en particulier lorsque les traitements sont automatisés. Cela permettra d'assurer une plus grande efficacité (notamment du fait qu'un tel conseiller connaîtra mieux l'organisation au sein de laquelle il travaille) et facilitera les contacts avec le préposé fédéral. Cela doit contribuer également à décharger le préposé de questions qui peuvent facilement être résolues au sein d'un office. Dans cette optique, l'article 23 prévoit la mise en place d'un conseiller à la protection des données auprès de chaque département et auprès de la Chancellerie fédérale.

La tâche première est celle d'un conseiller chargé d'orienter les utilisateurs en matière de protection des données. Contrairement au conseiller indépendant au sens de l'article 11a, alinéa 5, lettre e LPD, il n'a en principe pas de tâche de contrôle ou de représentation vers l'extérieur (par exemple, traitement des demandes d'accès). Toutefois, les unités administratives ont tout le loisir d'étendre son cahier des charges et de lui confier des tâches de contrôle et de représentation. De même, les départements et les offices sont libres de désigner plusieurs conseillers. Il est d'ailleurs souhaitable de

prévoir un tel conseiller dans les offices qui traitent des données sensibles ou des profils de la personnalité, ou qui gèrent de gros systèmes de traitement des données. Plusieurs offices l'ont déjà fait.

Conformément à l'article 23, alinéa 1, OLPD, les tâches du conseiller seront donc avant tout et essentiellement des tâches de conseil, de promotion et de formation. Ce conseiller devra être pour les autres collaborateurs de son office ou de son département, celui qui disposera des connaissances nécessaires en matière de protection et de sécurité des données, qui renseignera et contribuera au niveau interne à la mise en oeuvre des dispositions de protection des données. Il n'est en aucun cas un agent de liaison du préposé fédéral, mais il doit néanmoins être pour ce dernier la personne de contact. L'alinéa 3 prévoit d'ailleurs que les organes fédéraux communiquent avec le préposé par l'intermédiaire de leur conseiller.

Si les départements ou la Chancellerie entendent être déliés de leur devoir d'annonce des fichiers en vertu du nouvel article 11a, alinéa 5, lettre e, LPD, ils doivent désigner un conseiller indépendant. Dans ce cas, les articles 12a et 12b lui sont applicables (art. 23, al. 2).

8. Dispositions particulières (art. 24 à 27a OLPD)

8.1 Collecte de données (art. 24)

Cette disposition concrétise le postulat d'une meilleure transparence lors du traitement de données personnelles, notamment par l'information qui doit être prodiguée aux personnes concernées. Elle complète les articles 4, 7a et 18 LPD). Il n'est en effet pas rare que des données soient collectées systématiquement à l'aide de questionnaires et de manière facultative, notamment à des fins statistiques. Il est alors normal que la personne interrogée puisse savoir si elle doit répondre ou non, et quelles sont les conséquences en cas de refus ou de réponse inexacte.

8.2 Numéro personnel d'identification (art. 25)

Le numéro personnel d'identification est un instrument unique pour identifier une personne dans un fichier public déterminé. Ce numéro d'identification peut être réservé à un domaine spécifique ou servir d'identifiant universel ou à usages multiples. Il peut être signifiant, c.à.d. comporter des informations codées (par ex. nom, sexe, état civil, nationalité) ou non signifiant, à savoir être formé de caractères choisis au hasard. En règle générale, les organes fédéraux devraient opérer avec des numéros non signifiants. Le numéro d'identification doit ainsi être considéré comme une donnée personnelle.

Le recours à un tel numéro revêt des avantages et des désavantages. Il permet en particulier une plus grande exactitude et peut être un facteur d'efficacité et d'économie (notamment si on utilise un seul numéro dans toute l'administration). Il permet en effet d'éviter la confusion entre homonymes, de contrôler l'exactitude ou la fiabilité des informations d'un fichier en les comparant avec d'autres données. Par contre, le numéro d'identification facilite la connexion des fichiers, ce qui entraîne une augmentation des risques de profils de la personnalité étendus et accroît l'emprise de l'Etat sur les administrés. Psychologiquement, l'usage d'un numéro unique peut s'avérer dangereux, le citoyen se sentant réduit à l'état de simple numéro et exclu du processus de traitement des données, ce qui constituerait une atteinte à la dignité humaine et au droit à l'autodétermination individuelle en matière d'information: un organe étatique n'ayant plus besoin de contacter une personne concernée pour collecter ou vérifier des données. Enfin, le numéro d'identification peut faciliter la désanonymisation des données conservées et utilisées à des fins statistiques.

Conscient de ces risques, le législateur a confié au Conseil fédéral le soin de réglementer l'usage du numéro d'identification personnel (art. 36, al. 4 let. c) et de limiter l'usage de moyens d'identification traditionnels, tel le numéro AVS. Ainsi l'article 25 régit l'utilisation de numéros d'identification par les organes fédéraux, à l'exception du numéro AVS qui est régi par la législation spéciale.

Afin d'éviter qu'un numéro d'identification personnel nouvellement créé soit un numéro parlant favorisant la diffusion non désirée par la personne concernée de données personnelles telles que son état civil, son âge, son sexe, ainsi que son statut de national ou d'étranger, l'organe fédéral concerné choisira un identifiant non signifiant. Ce dernier doit en outre être réservé au champ d'activité pour

lequel il a été constitué, essentiellement pour prévenir les risques d'interconnexions indésirables (art. 25, al. 1).

La création d'un tel numéro n'est pas seulement effectuée lors de la réalisation d'un nouveau fichier, mais également, dans les cas où les conditions du 1er alinéa ne sont pas remplies, lorsqu'un organe est appelé à restructurer des fichiers existants dans une mesure lui permettant de changer de numéro. Ainsi, peu à peu, un identifiant tel que le numéro AVS pourra être remplacé par un numéro propre à un domaine spécifique.

L'article 25, alinéas 2 et 3, vise également à prévenir les risques d'interconnexions et les atteintes à la protection des données susceptibles d'en découler. Il permet à l'organe qui émet un numéro d'identification d'en contrôler l'usage, aussi bien par d'autres organes que par des personnes privées. Conformément aux principes de finalité et de compatibilité des buts, l'organe concerné ne donnera son accord à l'utilisation de son numéro d'identification que si l'utilisation prévue est en étroite connexité avec le domaine pour lequel le numéro d'identification personnel a été émis.

8.3 Communication des données (art. 26)

Voir commentaire sous point 6.1.5 ci-dessus.

8.4 Essais pilotes (art. 27, 27a)

8.4.1 Procédure (art.27)

L’article 17a LPD confère au Conseil fédéral la faculté d’autoriser, avant l’entrée en vigueur d’une loi au sens formel, le traitement automatisé de données sensibles et de profils de la personnalité dans le cadre d’essais pilotes, si certaines conditions cumulatives sont réalisées. La première de ces conditions est fixée à l’article 17a, alinéa 1, LPD qui prescrit que le préposé doit être consulté. Pour mettre en oeuvre cette disposition, il convient dès lors de régler dans l’ordonnance les modalités applicables.

Lorsqu’un organe fédéral envisage un essai pilote, l’article 27 prescrit à l’alinéa 1 qu’il doit communiquer au préposé de quelle manière il prévoit de respecter les exigences de l’article 17a LPD et l’inviter à prendre position. Le préposé prend position avant la consultation des unités administratives concernées.

Pour permettre au préposé de prendre position, l’organe fédéral responsable doit lui remettre les documents qui sont énumérés à l’alinéa 2. En vertu de cette disposition, il ne peut donc se limiter à alléguer de manière générale et abstraite que l’article 17a LPD s’applique au cas d’espèce. Il lui incombe au contraire d’exposer de manière exhaustive et concrète de quelle manière il prévoit de respecter chacune des conditions fixées à l’article 17a LPD. Les documents fournis par l’organe fédéral responsable doivent permettre au préposé de prendre position en connaissance de cause. Conformément à l’alinéa 3, le préposé peut exiger d’autres documents et procéder à des vérifications complémentaires.

Dans le cadre de sa prise de position, le préposé doit examiner si les conditions de l’article 17a sont réalisées. Une prise de position abstraite et succincte ne suffit pas. Il faut au contraire que le préposé prenne expressément position sur chacune des conditions prévues à l’article 17a LPD, en se référant, le cas échéant, aux explications fournies par l’organe fédéral responsable. Cette prise de position doit permettre à ce dernier d’adapter, si nécessaire, son projet d’essai pilote, avant de l’envoyer en procédure de consultation des offices concernés.

Si l’organe fédéral responsable modifie le projet d’essai pilote sur des points essentiels relatifs aux conditions de l’article 17a LPD, notamment après la consultation des unités administratives, il informe le préposé et l’invite le cas échéant à prendre à nouveau position (al. 4). Cette mesure se justifie par le fait que la prise de position du préposé est jointe à la proposition au Conseil fédéral et ne saurait donc porter sur un projet qui a été modifié entre-temps.

Une fois que le projet d’essai pilote est définitif, l’organe fédéral responsable trans-met à son département la proposition adressée au Conseil fédéral. La prise de position du préposé doit être jointe à cette proposition (al. 5). Il ne suffit donc pas de mentionner dans la proposition au Conseil fédéral que le préposé est d’accord avec le projet.

Il convient enfin de relever que le Conseil fédéral peut régler les modalités du traitement automatisé par voie d'ordonnance en même temps qu'il autorise l'essai pilote ou le faire après qu'il a autorisé un tel traitement. Les deux cas de figure sont donc possibles. Il y a lieu également de noter que la durée de validité de l'ordonnance d'exécution devra être expressément limitée à cinq ans (art. 17a, al. 5, LPD).

8.4.2 Rapport d'évaluation de l'essai pilote (art. 27a)

L'article 27a contient une règle de procédure relative à l'article 17a, al. 4 LPD qui prévoit l'obligation pour l'organe fédéral responsable de soumettre au Conseil fédéral un rapport d'évaluation ainsi que des propositions relatives à la poursuite ou à l'interruption du traitement, dans un délai de deux ans. Vu que la prise de position du préposé est communiquée au Conseil fédéral lors de l'autorisation de l'essai pilote, ce dernier doit également être informé de l'avis du préposé dans le cadre de la procédure relative au rapport d'évaluation.

9. Registre des fichiers et enregistrement (art. 28)

Aux termes de l'article 11a de la LPD, le préposé fédéral tient un registre des fichiers accessibles sur Internet. Ce registre recense l'ensemble des fichiers détenus par les organes fédéraux et les fichiers du secteur privé qui contiennent des données sensibles ou des profils de la personnalité faisant l'objet d'un traitement régulier ou qui contiennent des données faisant l'objet d'une communication régulière à des tiers. Ces fichiers doivent être déclarés à moins qu'ils ne soient couverts par une des exceptions de l'article 11a, alinéa 5 LPD et des articles 4 et 18 OLPD. Le Conseil fédéral règle les modalités de la déclaration et la tenue du registre.

L'article 28 détermine le contenu du registre et les modalités de sa publication. Le registre des fichiers est conçu comme un instrument permettant d'assurer la publicité des fichiers (principe de la transparence) en vue notamment de faciliter l'exercice du droit d'accès par les personnes concernées. Bien qu'il soit également un instrument fondamental pour permettre au préposé fédéral d'accomplir ses tâches de surveillance et de conseil, le registre doit contenir uniquement les données nécessaires à la finalité de publicité, c.à.d. donner une information suffisante sur le contenu et l'importance du fichier ainsi que ses finalités. Ainsi, le registre contient uniquement les informations qui sont contenues dans l'annonce des fichiers conformément à l'article 11a LPD et aux articles 3 et 16 OLPD, à savoir:

- nom et adresse du maître du fichier;
- nom et dénomination complète du fichier;
- personne ou organe auprès duquel peut être exercé le droit d'accès;
- base juridique et but du fichier (la base juridique informe sur la légitimité du fichier: elle concerne uniquement des fichiers des organes fédéraux);
- catégorie des données traitées (la catégorie des données traitées donne une indication sur les types de données enregistrées dans le fichier, par exemple nom, adresse, profession, date de naissance, etc.);
- catégorie de destinataires des données;
- catégorie de participants au fichier.

Les deux dernières catégories d'informations sont importantes pour permettre à la personne concernée de se faire une idée sur la nature du fichier (fichier isolé, fichier connecté ou ouvert). Cela lui permet également de suivre le cheminement des données la concernant et, le cas échéant, de s'adresser aux différents maîtres de fichier.

Lors de l'annonce, le préposé peut en outre exiger d'autres informations, conformément aux articles 27, alinéa 3 et 29, alinéa 2 LPD. Ces informations ne sont cependant ni enregistrées dans le registre des fichiers, ni publiées (voir également article 34 et paragraphe 10.3 ci-dessous).

Le registre est public et il est accessible en ligne. Sur demande, le préposé peut en outre communiquer gratuitement des extraits du registre (art. 28, al. 2 OLPD).

Une fois déclaré, le fichier doit être enregistré. La procédure d'enregistrement est régie par l'article 28, alinéa 4 OLPD. Selon l'article 11a, alinéa 4 LPD la déclaration intervient avant que le fichier soit opérationnel. Il n'y a pas de procédure d'autorisation, ni contrôle matériel de l'annonce. Le préposé procède à un examen sommaire afin de vérifier si la déclaration est complète. Une fois cet examen effectué, le préposé fédéral procède à l'enregistrement du fichier et à sa publication dans le registre des fichiers. Si l'annonce est incomplète le préposé invite le maître du fichier à s'acquitter de son obligation dans un délai déterminé. Passé ce délai, le préposé peut procéder d'office à l'enregistrement du fichier sur la base des informations en sa possession ou recommander la cessation du traitement.

L'enregistrement du fichier n'équivaut pas à un blanc-seing donné au maître du fichier. Le préposé peut être amené ultérieurement à constater qu'un traitement présente des lacunes du point de vue de la protection des données. Dans ces cas, et si le maître du fichier n'obtempère pas aux recommandations du préposé fédéral, celui-ci peut aller jusqu'à proposer au département concerné (art. 27 LPD) ou au Tribunal administratif fédéral TAF (art. 29 LPD) de prononcer la cessation du traitement et la radiation de l'enregistrement.

Aux termes de l'article 28, alinéa 3 OLPD, le préposé tient une liste des maîtres de fichiers qui sont déliés de leur devoir de déclarer leurs fichiers en vertu de l'article 11a, alinéa 5, lettres e et f, LPD (obtention d'un label de qualité en protection des données ou désignation d'un conseiller à la protection des données).

10. Préposé fédéral à la protection des données et à la transparence (art. 30 à 34 OLPD)

10.1 Statut, organisation et documentation (art. 30 à 32)

Les articles 30 à 32 complètent les dispositions de la LPD relatives au préposé fédéral et règlent en particulier les relations de service des membres du secrétariat du préposé, le siège et les relations avec les autres autorités. L'article 30, alinéa 3 prévoit en outre que le budget du préposé figure dans une rubrique spécifique du budget de la Chancellerie fédérale. Il s'agit d'une première concrétisation de l'article 26, alinéa 3, LPD qui prescrit que le préposé dispose de son propre budget. Ainsi, selon l'article 31, le préposé, qui est autonome, mais rattaché administrativement à la Chancellerie fédérale communique avec le Conseil fédéral par l'intermédiaire de la chancelière de la Confédération. Celle-ci a l'obligation de communiquer toutes les propositions ou rapports du préposé fédéral, même si elle ne peut y adhérer. Avec les autres autorités et les personnes privées soumises à la législation fédérale sur la protection des données ou celle sur le principe de la transparence de l'administration, le préposé fédéral communique directement.

Le préposé dispose également de sa propre documentation (art. 32). Les organes fédéraux doivent en particulier lui adresser tous leurs projets législatifs touchant le traitement de données personnelles et la protection des données, ainsi que ceux qui concernent le principe de la transparence de l'administration (accès aux documents officiels). De même en matière de protection des données, la Chancellerie fédérale et les départements communiquent au préposé leurs décisions, sous forme anonyme, et leurs directives. Cette information est nécessaire au préposé notamment pour faciliter ses activités de surveillance et de conseil auprès des organes fédéraux.

Pour améliorer l'efficacité et la rationalisation, le préposé fédéral est doté d'un système d'information automatisé propre pour la documentation, l'enregistrement des dossiers, le contrôle des affaires ou le registre des fichiers. Ce système lui permet également l'indexation et le contrôle de la correspondance et des dossiers, ainsi que la publication d'informations d'intérêt général. La documentation scientifique est mise à la disposition du Tribunal administratif fédéral. D'autres autorités et en particulier les conseillers à la protection des données des départements et des offices pourraient dans le futur bénéficier d'un tel accès.

10.2 Emoluments (art. 33)

A l'exception des avis que le préposé fédéral est appelé à émettre, aucun émolument n'est prélevé pour les activités de conseil et de surveillance du préposé, ceci pour tenir compte du fait que la procédure de déclaration et la surveillance du préposé exige une collaboration intensive des responsables des traitements. Il serait peu judicieux de les pénaliser en prélevant un émolument. Ainsi, l'enregistrement des fichiers, la déclaration de transferts à l'étranger ou les recommandations du préposé fédéral ne feront l'objet d'aucun émolument. Aucun émolument n’est prélevé auprès des autorités fédérales et cantonales.

10.3 Examen des traitements de données personnelles (art. 34)

Cette disposition énonce, à titre exemplatif, quels types d'informations complémentaires, le préposé peut être amené à demander au maître de fichier ou à l'organe responsable lorsqu'il examine la licéité d'un traitement ou la communication de données à l'étranger.

Certaines de ces informations pourront le cas échéant être collectées lors de l'annonce des fichiers ou la déclaration des flux transfrontières de données. Ces informations ne sont ni publiées, ni enregistrées dans le registre des fichiers.