Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

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

27 octobre 2009

# Guide pour l'élaboration des bases légales nécessaires pour exploiter un système de traitement automatisé de données personnelles

La présente note est principalement destinée aux juristes chargés d'élaborer les bases légales nécessaires pour pouvoir exploiter un système de traitement automatisé de données personnelles (ci-après système) conformément aux exigences de la loi fédérale sur la protection des données (LPD ; RS 235.1). Les questions préalables à se poser lors de la conception du système, avant même l'élaboration des bases légales sont traitées dans la première partie. L'élaboration des bases légales proprement dite est abordée dans la seconde partie, en particulier, les principes, le niveau auquel légiférer et la précision de la densité normative.

La présente note constitue un outil à prendre en compte lors de la mise en place d'un nouveau système de traitement. Il complète les méthodes et guides existants que l'organe fédéral responsable applique dans ce domaine, soit:

– la méthode de conduite et de déroulement de projets dans le domaine des technologies d'information et de la communication (HERMES) (http://www.hermes.admin.ch/welcome?set_language=fr&cl=fr),
– le guide pour la gestion électronique des affaires (GEVER http://www.bar.admin.ch/themen/00697/00791/index.html?lang=fr), ainsi que
– le guide pour l'élaboration de la législation fédérale (guide de législation de l'Office fédéral de la justice, http://www.bj.admin.ch/bj/fr/home/themen/staat_und_buerger/legistik/gesetzgebungsleitfaden.html).
– Les Directives de la Confédération sur la technique législative DTL, publiées par la Chancellerie de la Confédération suisse, 2003, www.bk.admin.ch/themen/gesetz/00050/index.

## A. Questions préalables

### 1 Caractéristiques des données

*1.1 Est-on en présence de données personnelles?*

La première question à se poser est de savoir si le système traitera des données personnelles au sens de la LPD, c'est-à-dire des informations qui se rapportent à une personne physique ou morale et qui permettent de l'identifier. La définition de

Office fédéral de la justice OFJ
Simone Füzesséry, Véronique Jaquet
Bundesrain 20, 3003 Berne
Tél. +41 31 322 47 59/41 41, Fax +41 31 322 84 01
simone.fuzessery@bj.admin.ch, veronique.jaquet@bj.admin.ch
www.ofj.admin.ch

*«données personnelles»* est très large puisqu'elle comprend toute information se rapportant à une personne identifiée, mais également à une personne identifiable. Par exemple, des données collectées sur «*le plus grand joueur suisse de tennis*» constituent des données personnelles car elles permettent d'identifier la personne concernée sans que son identité soit mentionnée. En revanche, des informations sur les différents types de fausse monnaie ne constituent pas des données personnelles.

Si le système ne traite pas de données personnelles, les exigences de la LPD ne sont pas applicables. La LPD vise en effet à protéger la personnalité des personnes physiques et morales et non les données comme telles.

Si la LPD ne s'applique pas au domaine concerné, autrement dit si ce dernier tombe dans une des exceptions au champ d'application de la LPD, tels que, par exemple, les registres publics relatifs aux rapports juridiques de droit privé, cela signifie uniquement que le législateur a considéré que le domaine concerné est régi par ses propres règles de protection des données. Le présent guide doit donc être pris en compte mutatis mutandis.

Bases légales : art. 1, 2, al. 2 et 3, let. a, LPD.

Exemples : l'art. 12, al. 3, let. a et c, de la loi sur les systèmes d'information de police de la Confédération (LSIP, RS 361) prévoit qu'un système contient des données relatives aux personnes annoncées à Fedpol en tant qu'auteurs présumés de délits, en tant que lésés ou dans le cadre de la recherche de personnes disparues.

### *1.2 Est-on en présence de données sensibles ou de profils de la personnalité?*

Si le système traite des données personnelles, il faut déterminer la nature de ces données, à savoir s'il s'agit de données sensibles ou des profils de la personnalité.

Par données sensibles, on entend les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, ainsi que des mesures d'aide sociale, des poursuites ou sanctions pénales et administratives. La définition est exhaustive.

Par profils de la personnalité, on entend un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique.

Ne constituent pas en revanche des données sensibles le nom d'une personne, sa date de naissance, les données patrimoniales (y compris les données sur les salaires).

Base légale : art. 3, let. a, c et d LPD.

Exemples: les données traitées selon l'art. 12, al. 3, let. a et c, LSIP précité au ch. 1.1 constituent des données sensibles.

### *1.3 Est-ce que la gravité de l'atteinte à la personnalité a été examinée?*

La gravité de l'atteinte à la personnalité doit être examinée en tenant compte non seulement de la nature des données, sensibles ou non, mais aussi, en particulier, du but du traitement (par exemple un fichier de police), de la manière de collecter les données (par exemple à l'insu de la personne concernée) du cercle et de l'étendue des personnes informées.

Exemple: Le Message du Conseil fédéral du 29 mai 2002 relatif à la loi fédérale sur le système d'information commun aux domaines des étrangers et de l'asile («Etrangers 2000 ») pose la question d'une future introduction de dossiers électroniques dans le domaine de l'asile et relève d'emblée qu'un tel système contiendrait «des données personnelles particulièrement sensibles (procès-verbaux d'audition, décisions d'asile, etc.) » (FF 2002 4367 [4382-4383]).

## 2 Finalité du système

### *2.1. Est-ce que la finalité générale du système est définie ?*

L'organe fédéral responsable est compétent pour décider du but du fichier. Il doit donc déterminer la finalité générale du système envisagé. Cette finalité doit être précise et reconnaissable pour la personne concernée. Il ne suffit pas qu'il envisage d'exploiter un système pour accomplir ses tâches légales.

Bases légales : art. 3, let. i et art. 4, al. 3 et 4 LPD.

Exemple : l'art. 14 LSIP prévoit que Fedpol exploite un système visant à l'identification dans le cadre de poursuites pénales et de la recherche de personnes disparues.

### *2..2 S'agit-il d'un système de gestion de dossiers interne ou d'un système d'information avec accès par procédure d'appel ?*

Une fois la finalité du système définie, il y a lieu de déterminer si le type de système envisagé correspond à un système de gestion de dossiers ou à un système d'information avec accès par procédure d'appel.

Par système de gestion, on entend un système d'information et de documentation visant à enregistrer, gérer, indexer et contrôler la correspondance et les dossiers. Dans un tel système, le maître du fichier ne peut enregistrer des données personnelles que dans le but de traiter les affaires de son ressort, d'organiser le déroulement du travail, de constater s'il traite des données se rapportant à une personne déterminée et de faciliter l'accès à la documentation. Seuls les collaborateurs de l'organe concerné ont accès à des données personnelles, et uniquement dans la mesure où ces données sont nécessaires à l'accomplissement de leurs tâches.

Lorsque plusieurs organes fédéraux exploitent le même système ou lorsque plusieurs organes fédéraux ou des tiers ont accès par procédure d'appel aux données traitées dans le système, il s'agit d'un système d'information dans lequel les communications sont établies en ligne selon le principe du «self service».

Il s'agit d'éviter, dans la mesure du possible, d'élaborer un système avec un caractère mixte (système de gestion de dossiers et d'information) à l'instar, par exemple, du système prévu pour l'entraide judiciaire internationale en matière pénale.

Bases légales : art. 57h de la loi sur l'organisation du gouvernement et de l'administration, (LOGA, RS 172.010) et art. 19, al. 3, LPD.

Exemple : l'art. 18 LSIP est consacré au système de gestion des affaires et des dossiers de Fedpol.

## 3 Architecture du système

### *3.1 Est-ce que l'architecture du système et ses potentialités sont clairement définies ?*

Lors de la conception d'un système, il est primordial d'instaurer dès le départ une collaboration entre les juristes et les informaticiens de l'organe fédéral responsable si l'on veut que les futurs textes législatifs correspondent à la réalité. Avant d'élaborer un projet de base légale, le juriste doit donc être en mesure, grâce à un dialogue avec les informaticiens responsables, de saisir l'architecture du système et ses potentialités. Il importe dans ce cadre de veiller à ce que le cadre juridique reflète fidèlement l'architecture informatique retenue et que les limites instaurées par le cadre juridique ne soient pas éludées par une architecture informatique au développement autonome.

### *3.2 Des sous-systèmes sont-ils prévus?*

Pour tenir compte du principe de la proportionnalité, il y a lieu de déterminer s'il est possible de créer des sous-systèmes.

Base légale : art. 4, al. 2, LPD.

Exemple : l'art. 5 de l'ordonnance sur le système informatisé de la Police judiciaire fédérale (ordonnance JANUS, RS 360.2) prévoit que le système JANUS est structuré en dix sous-systèmes.

### *3.3 Est-ce que des interfaces sont prévues avec d'autres systèmes d'information?*

Il s'agit de déterminer s'il est prévu de relier le système avec d'autres systèmes d'informations avec une interface.

Bases légales : art. 4, al. 2 et 19, al. 3 LPD.

Exemple : L'art. 9, al. 2, LSIP prévoit l'interconnexion des réseaux pour permettre aux utilisateurs disposant des droits d'accès nécessaires de savoir si une personne ou organisation figure dans un ou plusieurs systèmes du réseau des systèmes d'information de police.

### *3.4 Est-ce que des interfaces sont prévues avec un système central commun à différents Etats ?*

Il s'agit de déterminer si les données qui seront traitées dans le système seront transférées en ligne à un système central commun à différents Etats en particulier dans le cadre de la reprise et de la mise en œuvre de l'acquis Schengen/Dublin (voir à cet égard le manuel Procédure d'élaboration, de reprise et de mise en œuvre des développements de l'acquis de Schengen/Dublin).

Bases légales : les dispositions du traité international à mettre en œuvre ainsi que l'art. 19, al. 3, LPD.

Exemple: révision de la loi sur les étrangers en relation avec la mise en œuvre du Règlement (CE) n°767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'informations sur les visas (VIS) et l'échange de données entre les Etats membres sur les visas de court séjour (règlement VIS).

### *3.5 Est-ce qu'une interface avec le système des Archives fédérales est prévue?*

Lors de la conception du système, le versement aux Archives fédérales doit être examiné suffisamment tôt avec ces dernières afin d'adapter les particularités techni-

ques du système. L'archivage des données et documents digitaux de l'administration fédérale au sein des AFS fait en effet l'objet d'une mise en œuvre uniforme. (voir à cet égard http://www.bar.admin.ch/themen/00532/00536/index.html?lang=fr ainsi que ci-dessous ch. 10).

Bases légales : art. 7 de la loi sur l'archivage (LAr, RS 152.1) et art. 21 LPD.

## 4. Maître du fichier et éventuels tiers participants

### *4.1 Est-ce que le maître du fichier est identifié ?*

Il y a lieu de déterminer précisément le maître du fichier, c'est-à-dire l'organe fédéral responsable qui décidera du but et du contenu du fichier. Par organe fédéral, on entend l'autorité, le service fédéral ou une personne chargée d'une tâche de la Confédération. L'identification du maître du fichier est importante car il incombera à l'organe fédéral responsable de pourvoir à la protection des données personnelles qu'il traitera ou fera traiter dans l'accomplissement de ses tâches, de répondre aux demandes de renseignements issues de l'exercice du droit d'accès et d'effectuer les tâches de contrôle en s'assurant notamment que les données enregistrées dans le système sont traitées de manière licite et compatible avec les exigences légales de la protection des données et que la sécurité informatique est garantie.

Bases légales : art. 3, let. h et i, art. 8, 9 et art. 16, al. 1, LPD.

Exemple : l'art. 5 de la loi fédérale sur le système d'information commun aux domaines des étrangers et de l'asile (LDEA, RS 142.51) prévoit que l'ODM est responsable de la sécurité du système d'information et de la légalité du traitement des données personnelles. L'art. 6 de la loi précitée prévoit que les demandes visant à obtenir un droit d'accès à des données personnelles et celles visant à rectifier des données inexactes doivent être adressées à l'ODM et que les recours, régis par l'art. 25 LPD, doivent être adressés également à l'ODM.

### *4.2 Y a-t-il des tiers participants ?*

La question est de savoir si des tiers seront autorisés à introduire ou à modifier des données dans le système ou si, en d'autres termes, l'organe fédéral responsable traitera des données dans le système conjointement avec d'autres organes fédéraux ou cantonaux ou avec des tiers. La réponse à cette question permettra de déterminer clairement le rôle et la responsabilité de chaque participant en matière de protection des données.

Base légale : art. 16 LPD.

Exemple : l'art. 15 LSIP prévoit que Fedpol exploite un système de recherches informatisées de personnes et d'objets en collaboration avec les cantons.

## 5. Droit d'accès de la personne concernée

### *5.1 Est-ce que le droit d'accès de la personne concernée est garanti?*

Le droit d'accès de la personne concernée est un pilier fondamental de la protection des données. Il permet à la personne de prendre l'initiative de vérifier si des données la concernant sont traitées dans un système. L'exercice de ce droit peut conduire, en particulier, à la constatation du caractère illicite d'un traitement de données ou à la rectification de certaines données. Il y a lieu dès lors d'en tenir compte dès le début des travaux en déterminant précisément le maître du fichier auquel va s'adresser la

personne concernée et en organisant le système de manière à permettre à la personne concernée d'exercer son droit d'accès.

Bases légales : art. 8, 9 et 25 LPD.

Exemple: l'art. 7 LSIP distingue les demandes de renseignements à adresser à Fedpol, au Ministère public de la Confédération et à l'ODM.

### *5.2 Est-il nécessaire de prévoir des restrictions spécifiques au droit d'accès ?*

L'accès direct aux données doit, en principe, être garanti. A titre exceptionnel, la législation prévoit, dans certains domaines un droit d'accès indirect ou des restrictions spécifiques au droit d'accès. On se demandera s'il est nécessaire de prévoir ces restrictions du droit d'accès selon le domaine considéré en tenant compte de l'évolution dans ce domaine qui va dans le sens de limiter les restrictions au droit d'accès dans chaque cas d'espèce au strict nécessaire (cf. avis du Conseil fédéral sur la *motion 08. 3852 Leutenegger Oberholzer, Fichiers de la Confédération. Droit d'accès*).

Base légale : art. 9 LPD

Exemple: l'art. 18 de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI, RS 120) prévoit un droit d'accès indirect. L'art. 8 LSIP prévoit des restrictions spécifiques au droit d'accès applicable au système de traitement des données relatives aux infractions fédérales.

## 6. Accès en ligne

### *6.1 Est-il nécessaire de prévoir des accès en ligne ?*

Avant de créer une base légale, il y a lieu de déterminer si l'octroi d'un accès en ligne est indispensable au destinataire pour l'accomplissement de ses tâches légales. Un accès en ligne pour des raisons de commodité ne suffit pas. Un accès en ligne est accordé avec une certaine retenue, notamment lorsque la finalité du système est très différente de celle poursuivie par les futurs destinataires. Le cas échéant, l'accès doit être limité, dans la mesure du possible, aux données indispensables. Il est donc nécessaire d'envisager également des modes de communication de données autres que l'accès en ligne. Il peut s'agir de communication de documents papier sur demande dans un cas d'espèce (assistance administrative) ou d'office ou bien de communication électronique de certaines données, sans procédure d'appel (autrement dit sans principe du libre service).
Par exemple, la Directive du DFJP sur la mise en place de liaisons en ligne et l'octroi d'autorisations d'accès à des applications informatiques du DFJP (Directive du DFJP sur les liaisons en ligne) du 30 septembre 2004 pose des conditions strictes à la mise en place de procédures en ligne.

Bases légales : art. 4, al. 2 et 19, al. 3, LPD

Exemple: l'art 9 LDEA prévoit la possibilité pour l'Office fédéral des migrations d'accorder un accès en ligne par une procédure d'appel aux données relevant du domaine des étrangers à certaines autorités (par exemple au Corps des gardes-frontières) dans un but déterminé (pour les gardes-frontières, afin qu'ils puissent procéder à des contrôles d'identité et établir des visas exceptionnels). L'art. 13 LDEA prévoit que l'ODM peut communiquer des données sous forme de listes ou de fichiers électroniques à certaines autorités énumérées dans la loi ou à des tiers mandatés selon la loi. L'art. 14 LDEA permet à l'ODM de communiquer au cas par cas, des données personnelles sur demande écrite et dûment motivée par l'autorité qui les nécessite.

### *6.2 Est-ce que l'accès en ligne serait contraire à un important intérêt public ou à un intérêt légitime manifeste de la personne concernée ?*

L'organe fédéral responsable doit examiner si l'accès en ligne serait contraire à un important intérêt public ou à un intérêt légitime manifeste de la personne concernée.

Bases légales : art. 4, al 2 et 19, al. 3 et 4, let. a, LPD.

### *6.3 Est-ce que l'accès en ligne serait contraire à une obligation légale de garder le secret ou à une disposition particulière relevant de la protection des données ?*

L'organe fédéral responsable doit examiner si l'accès en ligne envisagé serait contraire à une obligation légale de garder le secret ou à des dispositions spécifiques de protection des données en vertu desquelles il serait tenu de refuser ou de limiter une communication de données même dans un cas d'espèce. Dans chaque domaine concerné, il y a donc lieu de déterminer si des dispositions spécifiques s'appliquent.

Base légale : art. 19, al. 3 et 4, let. b, LPD.

Exemple : l'art. 33 de la loi fédérale sur la partie générale du droit des assurances sociales (LPGA, RS 830. 1) impose une obligation de garder le secret aux personnes qui participent à l'application des lois sur les assurances sociales.

## 7. Exactitude des données

### *7.1 Est-ce que des mesures de contrôle de l'exactitude des données sont prévues ?*

Il incombe à l'organe fédéral responsable de s'assurer que les données qu'il traitera dans le système seront correctes. Il est d'ailleurs chargé de prouver l'exactitude des données traitées dans un système lorsqu'elle est contestée. Il convient par conséquent de déterminer, le cas échéant, en collaboration avec les informaticiens responsables, les mesures qui pourront être prises pour effacer ou rectifier les données inexactes ou incomplètes.

Base légale : art. 5 LPD.

Exemples : l'art. 16 de l'ordonnance sur le système d'information central sur la migration (ordonnance SYMIC, RS 142. 513) prévoit que l'ODM désigne un conseiller à la protection des données et à la sécurité informatique qui contrôle régulièrement l'exactitude et la sécurité des données. L'art. 15 de l'ordonnance JANUS charge notamment le service de contrôle de confirmer la saisie définitive des données enregistrées provisoirement après avoir vérifié leur exactitude. Par ailleurs, le jugement de la Commission fédérale de la protection des données du 7 avril 2003 (JAAC 67.73 consid. 4c) se penche sur le cas de l'exactitude d'une donnée figurant dans un système d'information contestée par le recourant et non démontrée par l'organe fédéral responsable.

## 8. Sécurité des données

### *8.1 Est-ce que des mesures techniques et organisationnelles pour garantir la sécurité des données sont prévues ?*

L'organe fédéral responsable doit, dès la conception du système, collaborer avec l'unité compétente de stratégie informatique de la Confédération pour prendre les mesures techniques et organisationnelles propres à garantir la protection des don-

nées personnelles. Il doit également annoncer son projet au Préposé fédéral à la protection des données et à la transparence ou au Conseiller à la protection des données qu'il a, le cas échéant, désigné.

Ces mesures doivent notamment tenir compte du but du traitement, de la nature et de l'étendue du traitement des données, de l'évaluation des risques potentiels pour les personnes concernées et du développement technique.

Les mesures prévues doivent protéger le système notamment contre les risques suivants :
– destruction accidentelle ou non autorisée ;
– perte accidentelle ;
– erreurs techniques ;
– falsification, vol ou utilisation illicite ;
– accès, modification, copie ou autre traitement non autorisés.

Bases légales : art. 7 LPD ; art. 8 et 20 OLPD.

### *8.2 Est-ce que des mesures particulières pour garantir la sécurité des données sont prévues ?*

Vu que l'organe fédéral responsable envisage un système de traitement automatisé de données personnelles, il doit prévoir des mesures particulières propres à réaliser notamment les objectifs suivants :
– contrôle à l'installation des entrées ;
– contrôle des supports de données personnelles ;
– contrôle du transport ;
– contrôle de communication ;
– contrôle de mémoire ;
– contrôle d'utilisation ;
– contrôle d'accès ;
– contrôle de l'introduction.

Le système devra être organisé de manière à permettre à la personne concernée d'exercer ses droits d'accès et de rectification.

Bases légales : art. 5, al. 2 LPD ; art. 9 OLPD.

### *8.3 Est-ce qu'un processus de journalisation doit être mis en œuvre ?*

L'organe fédéral responsable doit prévoir un processus de journalisation des traitements automatisés des données sensibles ou des profils de la personnalité en particulier lorsque les mesures préventives ne suffisent pas à garantir la protection des données. Une journalisation est notamment nécessaire, en cas de système complexe, lorsque, sans cette mesure, il n'est pas possible de vérifier a posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées. Elle pourra, selon les domaines, découler d'un traité international.

Bases légales : art. 10 de l'ordonnance relative à la loi fédérale sur la protection des données, (OLPD, RS 235. 11). Pour ce qui concerne la coopération policière, l'art. 10 de la décision-cadre sur la protection des données

traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO L 350/60 du 30.12. 2008), qui constitue un développement de l'acquis de Schengen à reprendre par la Suisse, prévoit une disposition d'application directe en matière de journalisation.

Exemple : l'art. 27 de l'ordonnance JANUS prévoit que tout traitement de données figurant dans JANUS est consigné dans un procès-verbal et que ces procès-verbaux sont conservés durant un an.

## 9 Tâches de l'administrateur du système, des services de contrôle et de maintenance

### *9.1 Est-ce que les tâches de l'administrateur du système, des services de contrôle et de maintenance sont définis ?*

L'étendue de l'accès au système de l'administrateur du système, des services de contrôle et de maintenance doit faire l'objet d'une réflexion préalable, et respecter le principe de proportionnalité

Base légale : art. 4, al. 2, LPD.

Exemple: l'art. 5 LSIP distingue l'accès des services de contrôle internes à l'administration chargés de vérifier l'application des dispositions relatives à la protection des données de celui des personnes chargées de la maintenance et de la programmation informatique. Pour ces derniers, le traitement de données est soumis, notamment, à la condition selon laquelle l'accomplissement de leurs travaux de maintenance et de programmation l'exige absolument.

## 10 Archivage des données

### *10.1 S'agit-il d'un système qui contiendra des données personnelles susceptibles d'avoir une valeur archivistique?*

Il y a lieu de déterminer si les données qui seront traitées sont susceptibles d'avoir une valeur archivistique et si elles devront être proposées aux Archives fédérales une fois que l'organe fédéral n'en aura plus besoin en permanence. Cet examen doit être effectué en collaboration avec les Archives fédérales qui disposent des ressources et des connaissances nécessaires pour analyser la valeur archivistique des données ainsi que pour toutes les questions techniques concernant l'archivage des données. Cette collaboration contribue à simplifier l'administration quotidienne des données. Elle évite une charge supplémentaire de travail lors de l'archivage ultérieur des données.

Bases légales : art. 21 LPD et art. 7 LAr.

### *10.2 Est-ce qu'un processus d'archivage a été prévu?*

L'organe fédéral responsable doit proposer aux Archives fédérales de reprendre toutes les données personnelles dont il n'a plus besoin en permanence.

Lors de la mise en œuvre d'un nouveau système, les juristes et les informaticiens de l'organe fédéral responsable doivent définir un processus d'archivage portant en particulier sur les questions suivants : quelles sont les mesures techniques prévues pour pouvoir ultérieurement verser les données personnelles aux Archives fédérales ? Est-ce qu'une interface avec le système des Archives fédérale est prévue ? Quand faudra-t-il leur proposer ces données? A quelle fréquence ? Quelles seront les données qui devront être proposées et de quelle manière ?

La mise en place d'un processus d'archivage est particulièrement importante en cas de migration des données d'un ancien système dans un nouveau système. Dans cette hypothèse, le processus d'archivage devra être appliqué avant l'entrée en fonction du nouveau système. Le fait que des données pourraient un jour être à nouveau utiles pour l'organe fédéral responsable, ne dispense pas ce dernier de l'obligation de prévoir un processus d'archivage.

Bases légales : art. 7 LAr et art. 21, al. 1, LPD; instructions du 13 juillet 1999 concernant la gestion de documents dans l'administration fédérale.

Exemple : l'art 6, al. 5 LSIP décrit la proposition aux Archives et la destruction des données et documents que les Archives fédérales jugent sans valeur archivistique.

## 11. Gestion, durée de conservation et destruction des données

### *11.1 Est-ce que le système prévu permet de respecter les prescriptions de la gestion électronique des affaires (GEVER) ?*

Conformément à la décision du Conseil fédéral du 23 janvier 2008, la Chancellerie fédérale et les départements doivent adopter la gestion électronique des affaires (GEVER) d'ici à la fin 2011. Dans cette perspective, les Archives fédérales proposent plusieurs documents d'informations et notamment le guide pour la gestion électronique des affaires.

Bases légales : art. 22 de l'ordonnance du 22 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA ; RS 192.010.1) ; instructions du 13 juillet 1999 concernant la gestion de documents dans l'administration fédérale.

### *11.2 Est-ce qu'un délai de conservation est prévu ?*

La durée de conservation de données personnelles doit être conforme au principe de proportionnalité. Une longue durée de conservation ne saurait être justifiée par le fait que les données personnelles pourraient un jour être à nouveau utiles pour l'organe fédéral responsable. Si la durée de conservation varie en fonction des catégories de données traitées, il y a lieu d'organiser le système de manière à pouvoir prévoir plusieurs délais de conservation, en créant par exemple des sous-systèmes.

Base légale : art. 4, al. 2, LPD.

Exemples : l'art 45, al. 2 de l'ordonnance sur la partie nationale du Système d'information Schengen (N-SIS) et sur le bureau SIRENE, (ordonnance N-SIS, RS 362.0) prévoit que certaines informations sont effacées au plus tard un an après que le signalement de la personne concernée a été effacé du SIS. L'art. 6 LSIP prévoit différentes procédures d'effacement des données selon qu'il s'agisse de données saisies isolément ou de données liées entre elles, effacées en bloc. Il distingue la conservation, l'effacement, l'archivage et la destruction des données.

### *11.3 Est-ce qu'un processus de destruction est prévu ?*

Si les Archives fédérales considèrent que les données personnelles proposées par l'organe fédéral responsable n'ont pas de valeur archivistique, ce dernier est tenu de les détruire, à moins que ces données ne soient rendues anonymes ou ne doivent être conservées à titre de preuve ou par mesure de sûreté.

Base légale : art. 21, al. 2, LPD.

## 12 Responsabilité civile en cas de dommage

### *12.1 Est-ce que la question de la responsabilité en cas de dommage a été approfondie ?*

Il s’agit finalement de s’interroger sur la question de la responsabilité en cas de dommage causé par un traitement illicite de données. Cette question se distingue de celle de la responsabilité pour la protection des données.

Base légale : voir en particulier, l’art. 3 de la loi sur la responsabilité (RS 170.32).

Exemple : l’art. 51 de l’ordonnance N-SIS rappelle que la responsabilité en cas de dommages liés à l’exploitation du système se fonde sur les art. 19*a* à 19*c* de la loi sur la responsabilité.

**Check-liste des questions à examiner lors de la conception du système**

| | |
|---|---|
| **1. Caractéristiques des données** | |
| 1.1 Est-on en présence de données personnelles? | ☐ Non -> LPD pas applicable.<br>☐ Oui |
| 1.2. Est-on en présence de données sensibles ou de profils de la personnalité? | ☐ Non<br>☐ Oui |
| 1.3 La gravité de l'atteinte à la personnalité a-t-elle été examinée? | ☐ Non<br>☐ Oui |
| **2. Type de systèmes** | |
| 2.1 Est-ce que la finalité générale du système est définie ? | ☐ Non<br>☐ Oui |
| 2.2 S'agit-il d'un système de gestion de dossiers interne ou d'un système d'information avec accès par procédure d'appel ? | ☐ système de gestion de dossiers interne<br>☐ système d'information avec accès par procédure d'appel |
| **3. Architecture du système du système** | |
| 3.1 Est-ce que l'architecture du système et ses potentialités sont clairement définies ? | ☐ Non<br>☐ Oui |
| 3.2 Des sous-systèmes sont-ils prévus? | ☐ Non<br>☐ Oui |
| 3.3 Est-ce que des interfaces sont prévues avec d'autres systèmes d'information? | ☐ Non<br>☐ Oui |
| 3.4 Est-ce que des interfaces sont prévues avec un système central commun à différents Etats ? | ☐ Non<br>☐ Oui |
| 3.5 Est-ce qu'une interface avec le système des Archives fédérales est prévue? | ☐ Non<br>☐ Oui |
| **4. Maître du fichier et éventuels tiers participants** | |
| 4.1 Est-ce que le maître du fichier est identifié ? | ☐ Non<br>☐ Oui |

| | |
|---|---|
| 4.2 Y a-t-il des tiers participants ? | ☐ Non<br>☐ Oui |
| **5. Droit d'accès de la personne concernée** | |
| 5.1 Est-ce que le droit d'accès de la personne concernée est garanti ? | ☐ Non<br>☐ Oui |
| 5.2 Est-il nécessaire de prévoir des restrictions spécifiques au droit d'accès? | ☐ Non<br>☐ Oui |
| **6. Accès en ligne** | |
| 6.1 Est-il nécessaire de prévoir des accès en ligne ? | ☐ Non<br>☐ Oui |
| 6.2 Est-ce que l'accès en ligne serait contraire à un important intérêt public ou à un intérêt légitime manifeste de la personne concernée ? | ☐ Non<br>☐ Oui |
| 6.3 Est-ce que l'accès en ligne serait contraire à une obligation légale de garder le secret ou à une disposition particulière relevant de la protection des données ? | ☐ Non<br>☐ Oui |
| **7. Exactitude des données** | |
| 7.1 Est-ce que des mesures de contrôle de l'exactitude des données sont prévues ? | ☐ Non<br>☐ Oui |
| **8. <u>Sécurité des données</u>** | |
| 8.1 Est-ce que des mesures techniques et organisationnelles pour garantir la sécurité des données sont prévues ? | ☐ Non<br>☐ Oui, contre les risques suivants :<br>☐ destruction accidentelle ou non autorisée ;<br>☐ perte accidentelle ;<br>☐ erreurs techniques ;<br>☐ falsification, vol ou utilisation illicite ;<br>☐ accès, modification, copie ou autre traitement non autorisés ;<br>☐ autres risques : … |

| | |
|---|---|
| 8.2 Est-ce que des mesures particulières pour garantir la sécurité des données sont prévues ? | ☐ Non<br>☐ Oui, pour réaliser les objectifs suivants :<br>☐ contrôle à l'installation des entrées ;<br>☐ contrôle des supports des données personnelles ;<br>☐ contrôle du transport ;<br>☐ contrôle de communication ;<br>☐ contrôle de mémoire ;<br>☐ contrôle d'utilisation ;<br>☐ contrôle d'accès ;<br>☐ contrôle de l'introduction ;<br>☐ autres objectifs. |
| 8.3 Est-ce qu'un processus de journalisation doit être mis en œuvre ? | ☐ Non<br>☐ Oui |
| **9. Tâches de l'administrateur du système** | |
| 9.1 Est-ce que les tâches de l'administrateur du système, des services de contrôle et de maintenance sont définies? | ☐ Non<br>☐ Oui |
| **10 Archivage des données** | |
| 10.1 S'agit-il d'un système qui contiendra des données personnelles susceptibles d'avoir une valeur archivistique? | ☐ Non<br>☐ Oui |
| 10.2 Est-ce qu'un processus d'archivage a été prévu? | ☐ Non<br>☐ Oui |
| **11. Gestion, durée de conservation et destruction des données** | |
| 11.1 Est-ce que le système prévu permet de respecter les prescriptions de la gestion électronique des affaires (GEVER) ? | ☐ Non<br>☐ Oui |
| 11.2 Est-ce qu'un délai de conservation est prévu ? | ☐ Non<br>☐ Oui |
| 11.3 Est-ce qu'un processus de destruction est prévu ? | ☐ Non<br>☐ Oui |
| **12. Responsabilité civile en cas de dommage** | |
| 12.1 Est-ce que la question de la responsabilité en cas de dommage a été approfondie ? | ☐ Non<br>☐ Oui |

Ce n'est qu'à ce stade que l'on pourra se demander ce qui doit figurer dans une loi au sens formel et ce qui peut figurer dans une base légale au sens matériel.

## B. Elaboration des bases légales

Les art. 17 et 19 LPD fixent certaines exigences concernant les bases juridiques applicables aux traitements de données personnelles effectués par les organes fédéraux. En principe, un organe fédéral n'est en droit de traiter et de communiquer des données personnelles que s'il existe une base légale (art. 17, al. 1, et 19, al. 1, LPD). Une base légale au sens formel est exigée s'il s'agit de données sensibles ou des profils de la personnalité (art. 17, al. 2, LPD). Lorsque l'organe fédéral rend des données personnelles accessibles en ligne, une base légale est toujours exigée. S'il s'agit de données sensibles ou de profils de la personnalité, une loi au sens formel doit le prévoir expressément (art. 19, al. 3, LPD).

Lorsqu'un organe fédéral gère un système de gestion de dossiers interne, l'art. 57*h* LOGA constitue la base légale applicable. Cette disposition règle la nature des données, la finalité des traitements et les droits d'accès internes. En vertu de l'al. 3, le Conseil fédéral édicte des dispositions d'exécution sur l'organisation et l'exploitation de ces systèmes d'information et de documentation ainsi que sur la protection des données personnelles qui y sont enregistrées.

Au vu de ces dispositions, une base légale au sens formel est nécessaire si l'organe fédéral responsable envisage d'exploiter un système d'information avec accès par procédure d'appel à des données sensibles. Si l'organe fédéral responsable ne prévoit pas de traitements de données sensibles ou de profils de la personnalité ni d'accès par procédure d'appel à ce type de données, une loi au sens matériel suffit.

A noter que l'art. 17*a* LPD consacré au traitement de données automatisé dans le cadre d'essais pilotes ne vise pas à suppléer à l'absence de base légale au sens formel. Cette disposition permet uniquement de tester un système d'information avant de définir le contenu permanent de la loi lorsque toutes les conditions posées par cette disposition sont remplies.

Selon le guide pour l'élaboration de la législation fédérale et la directive de l'Office fédéral de la justice sur la présentation d'esquisses d'acte normatif pour les projets législatifs relevant de la compétence de cet office (http://intranet.bj.admin.ch/inbj-publ/bj/fr/home/weisungen.html), il convient de déterminer le contenu important de la réglementation à adopter avant de rédiger un projet de loi. Selon la directive de l'Office fédéral de la justice, cette étape correspond à l'élaboration d'une esquisse d'acte normatif qui doit contenir les éléments suivants : résumé du contenu normatif, structure générale de l'acte, forme de l'acte, niveau des normes, normes de délégation, densité normative.

### 1. Résumé du contenu de l'acte

Il convient en premier lieu de résumer le contenu normatif essentiel de la réglementation à adopter. Ce résumé peut être présenté sous forme de thèses ou de principes directeurs qui fixent l'identité du maître du fichier, la finalité du système, le droit d'accès de la personne concernée, le type de traitements, la nature des données et les éventuels accès en ligne. Il s'agit en fait d'un résumé des réponses aux questions formulées en première partie de la présente note.

## 2. Structure générale de l’acte

Il y a lieu de définir la structure générale de l’acte. La réglementation pour un système d’information contiendra les sections suivantes : les dispositions générales incluant la finalité du système et son architecture, le traitement des données personnelles, l’accès par procédure d’appel, la communication de données personnelles, les dispositions d’exécution et les dispositions finales.

## 3. Forme de l’acte

Il y a lieu de déterminer la forme de l’acte à adopter en examinant en particulier la question de savoir s’il faut adopter un nouvel acte ou modifier un acte en vigueur.

On se posera également à ce stade la question de savoir s’il convient d’élaborer un texte législatif consacré uniquement aux systèmes d’informations ou si ces dispositions peuvent être intégrées dans un acte législatif traitant du domaine concerné. On prendra soin dans ce cadre de ne pas déséquilibrer une loi en insérant un ensemble de dispositions sur un système d’information. Le cas échéant, il conviendrait de recourir à une loi séparée, consacrée à la réglementation du système d’information.

Exemples : la loi sur le système d’information commun aux domaines des étrangers et de l’asile constitue un acte séparé, de même que la loi fédérale sur les systèmes d’information de l’armée, FF 2008 7505.

## 4. Niveau de l’acte

Il y a lieu de déterminer le niveau des normes et en particulier si des normes de délégations doivent être prévues. Le niveau normatif dépend de la gravité de l’atteinte à la personnalité des personnes concernées. Dans le cadre de la délégation législative, il s’agit de distinguer la délégation d’édicter des règles primaires (i.e. des règles qui complètent la loi et qui ne se limitent pas à la concrétiser) de celle d’édicter des règles secondaires, autrement dit, des dispositions d’exécution proprement dites.

### *4.1 Au niveau d’une loi au sens formel*

Au niveau d’une loi au sens formel, il y a lieu de régler les points suivants :

– Le contenu du système d’information,
– la finalité du système d’information,
– L’architecture du système d’information,
– l’identité du maître du fichier,
– Les tiers-participants,
– Les éventuelles restrictions du droit d’accès de la personne concernée,
– Les catégories de données sensibles traitées,
– Les accès en ligne au système d’information,
– La communication de données sensibles ou de profils de la personnalité sans procédure d’appel,
– Une délégation législative d’édicter des règles primaires,
– Une délégation législative d’édicter des dispositions d’exécution.

### *4.2 Au niveau d'une ordonnance*

En fonction de la délégation législative prévue, il y aura lieu de régler, dans le cadre d'une ordonnance, les points suivants :

– Les détails de l'architecture du système d'information,

– Un catalogue des données traitées dans le système,

– Une précision quant au maître du fichier et son obligation, lecas échéant, d'édicter un règlement de traitement au sens de l'art. 21 OLPD.

– Un catalogue des données accessibles en ligne et les modalités de l'accès,

– Les modalités relatives au droit d'accès de la personne concernée,

– La responsabilité pour la protection des données de l'organe fédéral responsable et, le cas échéant, des tiers participants,

– Les mesures de protection techniques et organisationnelles,

– Le délai de conservation, l'effacement, l'archivage et la destruction des données.

## 5. Densité normative

Selon la jurisprudence du Tribunal fédéral, pour déterminer quel degré de précision («*densité normative*») on est en droit d'exiger d'une loi, il faut tenir compte du cercle de ses destinataires, et de la gravité des atteintes qu'elle autorise aux droits fondamentaux. Une atteinte grave exige en principe une base légale au sens formel, claire et précise, alors que les atteintes plus légères peuvent, par le biais d'une délégation législative, figurer dans des actes de niveau inférieur à la loi.

Exemple : ATF 123 I 112

### *5.1 Densité normative des dispositions à faire figurer dans une loi au sens formel*

Une base légale au formel pour le traitement et l'accès en ligne de données sensibles et de profils de la personnalité doit permettre en substance de répondre aux questions suivantes :

– Qui traite quelles catégories de données et dans quel but ?

– Qui a accès à quelles catégories de données et dans quel but ?

Par conséquent, pour les points à régler au niveau d'une loi au sens formel, la densité normative doit être la suivante :

– La finalité du système d'information : La finalité doit être définie de manière précise. Il ne suffit pas d'indiquer que le système a pour but de permettre à l'organe fédéral responsable d'accomplir ses tâches légales.

  Exemple : art. 3 LDEA.

– l'identité du maître du fichier : La disposition légale doit indiquer quel organe fédéral gère le système et est responsable de la sécurité du système et de la légalité du traitement des données. Cette indication doit permettre à la personne concernée de savoir auprès de quelle autorité elle peut faire valoir ses droits et en particulier son droit d'accès.

  Exemples : art. 2 et 5 LDEA.

– Les tiers-participants : Les tiers participants doivent être reconnaissables pour la personne concernée.

Exemple : art. 15 LSIP

– Les restrictions du droit d'accès de la personne concernée : Les restrictions prévues doivent être justifiées par un intérêt public ou privé prépondérant et respecter le principe de proportionnalité.

  Exemple : art. 8 LSIP.

– Le contenu du système d'information : Les catégories de données enregistrées doivent être définies. Il y a également lieu de préciser si le système contient des données sensibles ou des profils de la personnalité.

  Exemple : art. 4 LDEA

– L'architecture du système d'information : L'architecture du système doit être décrite dans ses grandes lignes. La disposition légale doit permettre à la personne concernée de comprendre l'organisation du système, s'il existe des sous-systèmes ou des interfaces avec d'autres systèmes.

  Exemple : art. 9 LSIP.

– Le traitement de données sensibles ou de profils de la personnalité : La disposition légale doit définir l'(les) autorité (s) compétente (s) pour traiter les données dans le système, les catégories des données traitées et la finalité du traitement. Elle doit permettre à la personne concernée de savoir quelle est l'autorité compétente, quelles données la concernant ont été traitées et la finalité du traitement.

  Exemples : art. 4 et 5 LSIP.

– L'accès en ligne : La disposition légale doit définir l'organe fédéral compétent pour accorder l'accès en ligne, les autorités auxquelles un accès en ligne peut être accordé, les catégories des données accessibles en ligne et la finalité de l'accès en ligne. La personne concernée doit pouvoir savoir précisément quelles sont les données la concernant qui sont accessibles par procédure d'appel, à quelles catégories de destinataires et dans quel but. Le principe de proportionnalité doit être respecté. Un accès en ligne ne peut pas être accordé seulement parce qu'il pourrait être utile pour une autorité. Il doit être nécessaire pour l'accomplissement de ses tâches légales.

  Exemples : art. 9 à 11 LDEA.

– La communication de données sensibles ou de profils de la personnalité : La disposition légale doit définir l'organe fédéral compétent pour communiquer les données, les autorités auxquelles les données peuvent être communiquées, les catégories de données et la finalité de la communication. La disposition légale doit également préciser s'il s'agit d'une communication spontanée ou d'une communication sur demande. Le principe de proportionnalité doit être respecté. Ainsi seules les données nécessaires pour l'accomplissement des tâches légales de l'autorité destinataire peuvent être communiquées.

  Exemples : art. 12 à 15 LDEA.

– Une délégation législative habilitant le Conseil fédéral à édicter des règles primaires: la disposition légale doit prévoir une délégation législative précise en faveur du Conseil fédéral. Elle doit définir le but, l'objet et l'étendue de la délégation. Il s'agit d'y recourir avec retenue.

  Exemple : art. 17 LDEA.

### *5.2 Densité normative des dispositions qui peuvent figurer dans une ordonnance*

Les éléments qui peuvent être réglés au niveau de l'ordonnance sont, en particulier, les suivants.

– Les détails de l'architecture du système d'information.
  Exemple : art. 3 de l'ordonnance du 12 avril 2006 sur le système d'information central sur la migration (Ordonnance SYMIC, RS 142.512).
– Un catalogue des données traitées dans le système.
  Exemple : art. 4 de l'ordonnance SYMIC.
– La responsabilité détaillée pour la protection des données de l'organe fédéral responsable et, le cas échéant, la responsabilité des tiers participants.
  Exemple : art. 7 de l'ordonnance N-SIS.
– Les modalités de l'accès en ligne, y compris la désignation précise des autorités des autorités ayant accès aux systèmes d'information.
  Exemple : art. 7 de l'ordonnance N-SIS.
– Les modalités de communication de certaines données sans procédure d'appel.
  Exemple : art. 9 et 10 de l'ordonnance 3 sur l'asile relative au traitement de données personnelles, RS 142.314.
– Les modalités concernant l'exercice du droit d'accès de la personne concernée.
  Exemple : art. 19 de l'ordonnance SYMIC.
– Les mesures de protection techniques et organisationnelles.
  Exemple : art. 16 et 17 de l'ordonnance SYMIC.
– Le délai de conservation, l'archivage et la destruction des données.
  Exemple : art. 18 de l'ordonnance SYMIC.