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

16 décembre 2010

Guide pour l'élaboration des bases légales nécessaires pour exploiter un système de traitement automatisé de données personnelles (en lieu et place de la version du 16 mars 2010)

Le présent guide est principalement destiné aux juristes chargés d'élaborer les bases légales nécessaires pour 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 (A. Définition du problème et recherche des solutions). L'élaboration des bases légales proprement dite est abordée dans la seconde partie, en particulier, les principes de protection des données et le niveau auquel légiférer (B. Esquisse d'acte normatif).

La présente note constitue un outil à prendre en compte lors de la mise en place d'un nouveau système de traitement. Il concerne spécifiquement les questions de protection des données en relation avec la mise en place d'un système et ne dispense pas le légiste d'effectuer une démarche de légistique matérielle et formelle telle qu'elle est préconisée par le Guide de législation, en particulier par le module *"loi"*.

Il convient également de se conformer:

– aux autres moyens auxiliaires en matière de légistique
– à la méthode de conduite et de déroulement de projets dans le domaine des technologies d'information et de la communication (HERMES)
– au guide pour la gestion électronique des affaires (GEVER).

A. Définition du problème et recherche des solutions

Dans le cadre de la démarche de légistique matérielle, il convient en règle générale d'effectuer un cycle de résolution de problèmes (Voir →Préparation des travaux et collecte des informations nécessaires [module loi]). Les éléments qui suivent peuvent constituer une aide à la définition du problème et à la recherche de solutions.

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

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 *«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 données sur 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 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?

Il y a lieu de définir la finalité du système envisagé de manière précise et reconnaissable pour la personne concernée. Il ne suffit pas d'envisager la mise en place d'un système pour permettre à l'organe fédéral compétent d'accomplir ses tâches légales. Il convient d'établir une liste de ces tâches, en principe exhaustive, ou au moins exemplative, lorsque le nombre restreint de destinataires, le caractère anodin des données échangées ou le manque de gravité de l'atteinte à la personnalité le justifient.

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

Exemple : l'art. 14, al. 1, 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 informatique

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

3.1.1 Généralités

Par «*architecture informatique*» on entend la structure générale inhérente à un système informatique, l'organisation des différents éléments du système et des relations entre les éléments.

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 les grandes lignes de l'architecture et des potentialités du système. Cette collaboration est à maintenir jusqu'à la fin du processus de conception du système, qui peut subir des changements techniques en cours de route.

3.1.2 Connections avec d'autres systèmes d'information

Une des questions centrales à résoudre est celle de savoir si le système d'information à régler va avoir des connections avec d'autres systèmes d'information réglés ailleurs.

Exemple : L'art. 9, al. 2, LSIP prévoit l'interconnexion des systèmes 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.

Les termes utilisés dans la législation en vigueur sont ceux d'*«interconnexion»*, d'«interface», de *«transfert de données dans d'autres systèmes d'information»*, de *«mise en réseau»* ou, parfois, de *«sous-systèmes»* ou de *«composantes»* d'un système.

Si un système d'information réglé dans une certaine loi est connecté à un autre système d'information réglé dans un texte normatif différent, l'interconnexion entre les deux systèmes nécessite une base légale spécifique.

Exemple : L'accès partiel des autorités cantonales de police et du Corps des gardes frontières au système qui permet de saisir des données sur les personnes ayant affiché un comportement violent lors de manifestations sportives (HOOGAN) prévu à l'art. 24a de la loi sur les mesures visant au main-

tien de la sûreté intérieure passe par *l'interface* du système d'information RIPOL (cf. art. 9, al. 5 de l'ordonnance sur les mesures de police administrative et les systèmes d'information de l'Office fédéral de la police, RS 120. 52).

En revanche, le système de recherches informatisées de police (RIPOL) prévu à l'art. 15 LSIP a une interface avec le système d'information commun aux domaines des étrangers et de l'asile (SYMIC, RS 142.51) sans que cette dénomination ne soit utilisée, Seules les conséquences de cette interconnexion sont décrites, à savoir *«que la recherche dans le SYMIC induit une consultation en ligne du RIPOL»* (art. 3, al. 2 de l'ordonnance SYMIC, RS 142.513).

Autre cas de figure, les données traitées dans un système national sont échangées 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 : art. 4, al. 2 et 19, al. 3 LPD ainsi que les dispositions du traité international à mettre en œuvre.

Exemple: La 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'information sur les visas (VIS) et l'échange de données entre les Etats membres sur les visas de court séjour (règlement VIS; FF 2009 7987).

Certaines dispositions légales règlent le «*transfert de données*» d'un système d'information vers d'autres systèmes.

Exemple: L'art. 12 de la loi sur le système d'information commun aux domaines des étrangers et de l'asile permet au DFJP d'autoriser les autorités cantonales compétentes à transférer certaines données du système précité dans leur propre système d'information.

Ou encore, la «*mise en réseau*» de différents systèmes d'information.

Exemple: l'art. 4, al. 2 de l'ordonnance sur le traitement des données dans l'administration fédérale des douanes, RS 631. 061, prévoit que si les mêmes données sont traitées par divers offices de l'AFD, les systèmes d'information correspondants peuvent être mis en réseau, pour autant que cela soit nécessaire à un traitement efficace des données.

Certaines dispositions légales prévoient la création de *«sous-systèmes»* ou de composantes du système en particulier lorsqu'il s'agit de limiter les droits d'accès ou de traitement des utilisateurs.

Base légale : art. 4, al. 2, LPD.

Exemple : les art. 2 et 5 de l'ordonnance sur le système informatisé de la Police judiciaire fédérale (ordonnance JANUS, RS 360.2) prévoient que le système JANUS est structuré en dix sous-systèmes. En revanche, le Conseil fédéral décrit la structure du système d'information du DFAE (traitant des données pour l'affectation du personnel à l'étranger et pour les transferts) comme comportant deux composantes, avec des droits d'accès et des finalités différentes (art. 4 de l'ordonnance sur le système d'information Tangram, RS 235.23).

3.2 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 techniques 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 leurs informations sur l’archivage digital 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, qui devra pourvoir à ce que le système d’information soit uniquement utilisé pour les buts légaux assignés et veiller à la protection des données dans son ensemble. 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 personnes privées. 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 Comment le droit d’accès de la personne concernée sera-t-il 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

Exemples: 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

Exemples: 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?

Dans la mesure où un accès en ligne entre en ligne de compte, il s'agit d'examiner si l'accès en ligne est 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?

Il est, en outre, nécessaire d'examiner si l'accès en ligne envisagé est 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 données 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 de l'ordonnance relative à la loi fédérale sur la protection des données, (OLPD, RS 235. 11).

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 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 OLPD. 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.

Il convient de relever qu'il y aura lieu d'examiner en temps voulu dans quelle mesure la question du contrôle interne et de la maintenance informatique d'un système de traitement de données devrait être réglée de manière générale dans la législation sur la protection des données.

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.

Il convient de relever qu’il y aura lieu d’examiner en temps voulu dans quelle mesure la question du processus d’archivage devrait être réglée de manière générale dans la législation sur la protection des données ou dans la législation sur l’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, FF 1999 4988.

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 (cf. ci-dessus, p. 1). 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 172.010.1) ; instructions du 13 juillet 1999 concernant la gestion de documents dans l'administration fédérale, précitées.

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.
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.

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

La check-liste qui suit résume les paragraphes précédents et permet de vérifier rapidement que l'ensemble des problèmes ont été résolus.

1. Caractéristiques des données	
1.1 Est-on en présence de données personnelles?	☐ Non -> LPD pas applicable. ☐ Oui
1.2. Est-on en présence de données sensibles ou de profils de la personnalité?	☐ Non ☐ Oui
1.3 La gravité de l'atteinte à la personnalité a-t-elle été examinée?	☐ Non ☐ Oui
2. Finalité du système	
2.1 Est-ce que la finalité générale du système est définie ?	☐ Non ☐ 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 ☐ système d'information avec accès par procédure d'appel
3. Architecture du système informatique	
3.1 Est-ce que l'architecture du système informatique et ses potentialités sont clairement définies?	☐ Non ☐ Oui
3.2 Est-ce qu'une interface avec le système des Archives fédérales est prévue?	☐ Non ☐ Oui
4. Maître du fichier et éventuels tiers participants	
4.1 Est-ce que le maître du fichier est identifié ?	☐ Non ☐ Oui
4.2 Y a-t-il des tiers participants ?	☐ Non ☐ Oui
5. Droit d'accès de la personne concernée	
5.1 Comment le droit d'accès de la personne concernée sera-t-il garanti?	☐ Non ☐ Oui
5.2 Est-il nécessaire de prévoir des restrictions spécifiques au droit d'accès?	☐ Non ☐ Oui

6. Accès en ligne	
6.1 Est-il nécessaire de prévoir des accès en ligne ?	☐ Non ☐ 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 ☐ 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 ☐ Oui
7. Exactitude des données	
7.1 Est-ce que des mesures de contrôle de l'exactitude des données sont prévues ?	☐ Non ☐ Oui
8. Sécurité des données	
8.1 Est-ce que des mesures techniques et organisationnelles pour garantir la sécurité des données sont prévues ?	☐ Non ☐ Oui, 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 ; ☐ autres risques.
8.2 Est-ce que des mesures particulières pour garantir la sécurité des données sont prévues ?	☐ Non ☐ Oui, pour réaliser les objectifs suivants : ☐ contrôle à l'installation des entrées ; ☐ contrôle des supports des données personnelles ; ☐ contrôle du transport ; ☐ contrôle de communication ; ☐ contrôle de mémoire ; ☐ contrôle d'utilisation ; ☐ contrôle d'accès ; ☐ contrôle de l'introduction ; ☐ autres objectifs.
8.3 Est-ce qu'un processus de journalisation doit être mis en œuvre ?	☐ Non ☐ Oui

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?	☐ Non ☐ 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 ☐ Oui
10.2	Est-ce qu'un processus d'archivage a été prévu?	☐ Non ☐ Oui
11.	**Gestion, durée de conservation et destruction des données**	
11.1	Est-ce que le système prévu per-met de respecter les prescriptions de la gestion électronique des affaires (GEVER) ?	☐ Non ☐ Oui
11.2	Est-ce qu'un délai de conservation est prévu ?	☐ Non ☐ Oui
11.3	Est-ce qu'un processus de destruction est prévu ?	☐ Non ☐ 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. Esquisse d'acte normatif

La préparation d'un projet de loi concernant l'exploitation d'un système de traitement automatisé de données personnelles nécessite l'élaboration d'une esquisse d'acte normatif.
Voir →Elaborer une esquisse d'acte normatif (module "loi") ainsi que la Directive sur la présentation d'esquisses d'acte normatif pour les projets législatifs de l'Office fédéral de la justice.

S'agissant d'un domaine particulièrement technique, il convient de détailler de la façon suivante les différentes rubriques de l'esquisse d'acte normatif.

1. Résumé du contenu de l'acte

Le résumé du contenu de l'acte normatif fixe, en particulier, 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

La structure générale de l’acte régissant un système d’information contiendra notamment les subdivisions 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.

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 et contenu normatifs

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 formelle est exigée s’il s’agit de données sensibles ou de 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 formelle doit le prévoir expressément (art. 19, al. 3, LPD). 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 matérielle suffit en principe. Le niveau normatif dépend cependant également de la gravité de l’atteinte à la personnalité des individus concernés.

Lorsqu’un organe fédéral gère un système de gestion de dossiers interne, l’art. 57*h* LOGA constitue la base légale applicable.

Une base légale formelle 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 ?

4.1 Contenu d'une loi formelle

La loi formelle doit régler en particulier les points suivants:

– La finalité du système d'information : Elle doit être définie de manière précise et reconnaissable pour la personne concernée. Plus les risques d'atteintes à la personnalité de celle-ci sont élevés, plus le degré de précision doit être élevé. Quelque soit la nature des données traitées, il ne suffit pas d'indiquer que le système a pour but de permettre à l'organe fédéral responsable d'accomplir ses tâches légales ; il faut également énumérer dans une liste les tâches pour lesquelles un traitement automatisé des données est prévu (cf. ci-dessus ch. 2.1).
  Exemple : art. 3 LDEA.

– L'identité du maître du fichier : La disposition légale doit indiquer quel organe fédéral 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 : Ils doivent être reconnaissables pour la personne concernée.
  Exemple : art. 15 LSIP.

– Le contenu du système d'information : Les catégories de données traitées 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.

– Les catégories de données sensibles ou les 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.

– Les éventuelles restrictions au 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.

– L'architecture du système informatique : Elle 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.

– 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 elles le sont. 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 autori-

tés 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.

4.2 Contenu d'une loi matérielle

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

– Des précisions sur l'architecture du système d'information, (cf. ci-dessus ch. 3.1, il ne s'agit pas de régler les détails techniques mais bien de préciser la manière dont les données sont traitées et les interconnections éventuelles entre les différents systèmes d'information).

  Exemple : art. 3 de l'ordonnance SYMIC.

– Un catalogue des données traitées dans le système.

  Exemple : art. 4 de l'ordonnance SYMIC.

– Les détails de la responsabilité pour la protection des données de l'organe fédéral responsable et, le cas échéant, la responsabilité des tiers participants voire l'obligation pour le maître du fichier d'édicter un règlement de traitement au sens de l'art. 21 OLPD.

  Exemple : art. 7 de l'ordonnance N-SIS.

– Les modalités de l'accès en ligne, y compris la désignation précise 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.