Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la justice OFJ

Octobre 2018

Rapport explicatif concernant la loi fédérale mettant en œuvre la directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales

(Développement de l'acquis de Schengen)

Table des matières

1 Contexte

Le 15 septembre 2017, le Conseil fédéral a adopté le message concernant la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales[1]. Le projet a en particulier pour objectifs de:

- transposer les exigences de la directive (UE) 2016/680relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales (directive [UE] 2016/680)[2] en tant que développement de l'acquis de Schengen[3];
- mettre en œuvre les recommandations adressées par l'Union européenne à la Suisse lors de l'évaluation de 2014 dans le cadre de l'accord d'association à Schengen[4];
- rapprocher le droit fédéral des exigences du règlement (UE) 2016/679[5];
- reprendre les exigences du projet de modernisation de la convention STE 108 du Conseil de l'Europe[6] (« P-STE 108 »)[7].

Dans le cadre de ses travaux parlementaires, le Parlement a décidé de scinder le projet de révision totale de la LPD en deux étapes, afin de traiter en premier lieu les modifications nécessaires à la reprise de l'acquis de Schengen. Suite à cette décision, le Parlement a adopté, le 28 septembre 2018, la loi fédérale mettant en œuvre la directive (UE) 2016/680. Cet acte contient d'une part la loi fédérale sur la protection des données Schengen (LPDS). Elle modifie d'autre part les lois applicables aux domaines de coopération Schengen en matière pénale, en particulier le code pénal (CP)[8], le code de procédure pénale du 5 octobre 2007 (CPP)[9], la loi du 20 mars 1981 sur l'entraide pénale internationale (EIMP)[10], la loi fédérale du 22 juin 2001 sur la coopération avec la Cour pénale internationale (LCPI)[11], la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres Etats (LOC)[12], la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)[13] et la loi fédérale du 12 juin 2009 sur l'échange d'informations Schengen (LEIS)[14].

Quant à la révision totale de la LPD, les travaux parlementaires suivent leur cours. Une fois que le Parlement aura adopté la révision totale de la LPD, il est prévu d'abroger la LPDS au motif que les dispositions de cette loi feront double emploi avec celles de la future LPD.

---

1 FF **2017** 6565

2 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016, p. 89.

3 FF **2017** 6565 6611

4 FF **2017** 6565 6588

5 FF **2017** 6565 6618; Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1.

6 Projet de modernisation de la convention du Conseil de l'Europe STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

7 FF **2017** 6565 6616

8 RS **311**.0

9 RS **312.0**

10 RS **351.1**

11 RS **351.6**

12 RS **360**

13 RS **361**

14 RS **362.2**

2 Commentaire des dispositions de la LPDS

2.1 Préambule

La LPDS se fonde sur les dispositions suivantes de la Constitution fédérale[15]: l'art. 54, al. 1, qui confère à la Confédération une compétence législative dans le domaine des affaires étrangères, l'art. 123, qui lui confère une compétence législative en matière pénale, et l'art. 173, al. 2, qui attribue à l'Assemblée fédérale une compétence subsidiaire pour tous les objets qui relèvent de la compétence de la Confédération et qui ne ressortissent pas à une autre autorité fédérale.

La LPDS a pour objectif de transposer la directive (UE) 2016/680, qui constitue un développement de l'acquis de Schengen pour la Suisse. Selon l'art. 1, par. 1, de la directive, celle-ci établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces.

La directive (UE) 2016/680 remplace la décision-cadre 2008/977 JAI[16]. Cet acte fixait un certain nombre de principes de protection des données personnelles applicables aux domaines de la coopération judiciaire en matière pénale et de coopération policière mais uniquement par rapport aux échanges de données personnelles entre Etats Schengen (considérant 6). Comme il ressort du considérant 7 de la directive (UE) 2016/680, le législateur européen a considéré qu'il était essentiel d'assurer un niveau de protection des données élevé et homogène et de faciliter l'échange de données entre les autorités Schengen compétentes, afin de garantir l'efficacité de la coopération judiciaire en matière pénale et la coopération policière. Selon lui, le niveau de protection de la sphère privée des personnes concernées à l'égard du traitement des données les concernant par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, devrait être équivalent dans tous les Etats Schengen (considérant 7).

2.2 Dispositions générales

Art. 1 Objet

Al. 1, phrase introductive

L'al. 1 reprend le texte de l'art. 1, par. 1 de la directive (UE) 2016/680 sous réserve de deux différences. Contrairement à la directive (UE) 2016/680, les personnes concernées peuvent être des personnes physiques ou morales étant donné que la LPD protège les droits fondamentaux de ces deux catégories de personnes. La seconde différence est de nature rédactionnelle : la LPDS remplace les termes de "détection et enquêtes" par la notion d'"élucidation" des infractions pénales au motif que la distinction entre "détection" et "enquête" est peu claire.

Organes fédéraux assujettis à la LPDS

La question de savoir quels sont les organes fédéraux assujettis à la LPDS doit être examine au regard de la définition de la notion d « autorités compétentes » de l'art. 3 ch. 7 de la directive (UE) 2016/680. Selon cette norme et le considérant 11 de cet acte, cette notion vise

---

15 RS **101**

16 Décision-cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30.12.2008, p. 60.

d'une part les autorités publiques compétentes telles que les autorités judiciaires, la police ou d'autres autorités répressives (let. a) ainsi que tout autre organisme ou entité à qui le droit d'un Etat Schengen confie l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de la directive (UE) 2016/680 (let. b). Les organes fédéraux assujettis à la LPDS sont principalement les autorités pénales de la Confédération et les autorités fédérales compétentes en matière d'entraide judiciaire internationale en matière pénale. Selon le considérant 80 de la directive, celle-ci s'applique également aux traitements de données effectués par les juridictions nationales et autres autorités judiciaires dans l'exercice de leurs fonctions juridictionnelles, sous réserve de certaines dispositions. Les organes fédéraux concernés sont donc non seulement l'Office fédéral de la police (fedpol), l'OFJ en ce qui concerne le domaine de l'entraide judiciaire en matière pénale et le Ministère public de la Confédération mais aussi le Tribunal pénal fédéral, le Tribunal fédéral et les tribunaux cantonaux de contrainte, lorsqu'ils agissent au nom de la Confédération selon l'art. 2, al. 2, de la loi du 19 mars 2010 sur l'organisation des autorités pénales (LOAP)[17].

Par contre, la LPDS ne s'applique pas aux autorités cantonales. La directive (UE) 2016/680 lie également les cantons. Il incombe par conséquent aux législateurs cantonaux de transposer, si nécessaire, les nouvelles exigences européennes dans leurs législations[18].

Opérations de traitements assujettis au à la LPDS

La phrase introductive de l'art. 1, al. 1 définit la finalité des traitements des données qui tombent dans le champ d'application de la LPDS dans les mêmes termes que la directive (UE) 2016/680 sous réserve des deux modifications mentionnées ci-dessus. Selon le considérant 12, les activités menées par la police ou d'autres autorités répressives sont axées principalement sur la prévention et la détection des infractions pénales et les enquêtes et les poursuites en la matière, y compris les activités de police effectuées sans savoir au préalable si un incident constitue une infraction pénale ou non. Ces activités peuvent également comprendre l'exercice de l'autorité par l'adoption de mesures coercitives, par exemple lors de manifestations. Parmi ces activités figurent également le maintien de l'ordre public lorsque la mission est confiée à la police ou à d'autres autorités répressives lorsque cela est nécessaire à des fins de protection contre les menaces pour la sécurité publique et de prévention de telles menaces, qui sont susceptibles de déboucher sur une infraction pénale. Par contre, les activités relatives à la sécurité nationale, les activités des agences et des services responsables des questions de sécurité nationale ne sont pas considérées comme des activités relevant du champ d'application de la directive (UE) 2016/680 (considérant 14).

Au niveau fédéral, la LPDS s'applique dès lors que des données personnelles sont traitées par exemple dans le cadre de l'accomplissement des tâches légales de l'OFJ dans le domaine de l'entraide judiciaire internationale en matière pénale, dans le cadre des activités du domaine de direction coopération policière internationale de fedpol, des enquêtes de la police fédérale judiciaire dans les domaines relevant de la compétence de la Confédération ainsi que lors de l'échange d'informations de police avec les autorités de poursuite pénale d'autres pays, ou avec des organismes internationaux tels que INTERPOL et Europol, notamment dans les domaines du crime organisé, de la traite d'êtres humains et du trafic de migrants, de la pédocriminalité et de la pornographie illégale, de la cybercriminalité, des stupéfiants, du commerce illégal de biens culturels et de la fausse monnaie. Les activités du Ministère public de la Confédération tombent également dans le champ d'application de la LPDS, à savoir l'enquête et la poursuite des infractions énumérées aux articles 23 et 24 CPP et dans des lois fédérales spéciales.

---

17 RS **173.71**

18 FF **2017** 6565 6792

Par contre, les traitements de données personnelles effectués par le Service de renseignement de la Confédération ne tombent pas sous le coup de la LPDS (considérant 14 de la directive [UE] 2016/680). Il en va de même des traitements de données personnelles effectués dans les autres domaines de coopération Schengen (notamment visas, contrôles aux frontières et armes) qui ne relèvent pas de la directive (UE) 2016/680 et ne sont donc pas visés par la LPDS.

Al. 1, let. a

La LPDS s'applique aux traitements de données personnelles effectués par des organes fédéraux dans le domaine pénal dans le cadre de l'application de l'acquis de Schengen. La notion d'acquis de Schengen découle de l'accord d'association à Schengen (AAS)[19]. En l'espèce, il s'agit de l'ensemble des dispositions contenues dans les annexes A et B et de tous les développements que la Suisse est tenue, en vertu de l'art. 2, par. 3, AAS, d'accepter, de mettre en œuvre et d'appliquer concernant notamment l'échange d'informations et de données personnelles en matière de coopération policière et d'entraide judiciaire en matière pénale.

Dans la mesure où les organes fédéraux traitent des données personnelles pour les finalités définies à l'art. 1, par. 1, de la directive (UE) 2016/680 dans le cadre de l'application des dispositions de l'acquis de Schengen, ceux-ci sont tenus de traiter ces données conformément aux standards de protection des données de la directive (UE) 2016/680 et d'appliquer par conséquent la LPDS. Ces données bénéficient en quelque sorte d'un régime spécial de protection dans le cadre de l'accomplissement des tâches légales des organes fédéraux compétents. Ces données sont qualifiées « Schengen », non seulement lorsque les organes fédéraux les ont obtenues d'un Etat Schengen par les voies de communication du Bureau SIRENE, mais aussi lorsque les organes fédéraux les traitent ou les consultent dans un système d'information qui est créé sur la base d'un acte appartenant à l'acquis de Schengen. Tel est le cas par exemple lorsque ceux-ci traitent des données dans le système d'information Schengen (art. 16 LSIP) ou encore lorsque fedpol ou le Ministère public de la Confédération consultent le système d'information sur les visas (VIS) conformément à l'art. 109a de la loi fédérale du 16 décembre 2005 sur les étrangers[20].

La LPDS s'appliquera également aux futurs développements de l'acquis de Schengen dès que la Suisse les aura repris.

Let. b

La LPDS règle également les traitements de données personnelles effectués dans le domaine pénal en application d'accords internationaux conclus avec l'Union européenne ou avec des Etats Schengen et qui renvoient à la directive (UE) 2016/680 pour ce qui est de la protection des données personnelles. Cette disposition vise des accords qui ne constituent pas un développement de l'acquis de Schengen mais qui déclarent la directive (UE) 2016/680 applicable. Seuls des accords internationaux conclus entre la Suisse et l'Union européenne ou avec un Etat Schengen sont couverts par la let. b, à l'exclusion de tout autre traité conclu avec un Etat tiers.

L'al. 1, let. b, vise en particulier l'accord entre la Suisse et l'Union européenne en vue d'approfondir la coopération policière internationale ainsi que le protocole relatif à l'accès des autorités de poursuite pénale à la banque de données Eurodac.

---

19 RS **0.362.31**

20 RS **142.20**

Al. 2: accords d'association à Schengen

Cette disposition précise que les accords d'association à Schengen sont mentionnés en annexe.

Art. 2 Relation avec d'autres actes

Al. 1: droits des personnes concernées dans le cadre d'une procédure

Aujourd'hui, l'art. 2, al. 2, let. c, de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[21] prévoit que la loi ne s'applique pas notamment aux procédures pendantes pénales et d'entraide judiciaire internationale. Cette exception n'est pas compatible avec le champ d'application de la directive (UE) 2016/680 tel qu'il est défini aux art. 1 et 2. L'art, 2, al. 1 LPDS introduit dès lors une réserve concernant ces procédures mais qui se limite aux droits des personnes concernées, comme le permet l'art. 18 de la directive (UE) 2016/680. En vertu de cette disposition, et selon le considérant 49, lorsque les données à caractère personnel sont traitées dans le cadre d'une enquête pénale ou d'une procédure judiciaire en matière pénale, les Etats Schengen peuvent prévoir que les droits des personnes concernées, à savoir le droit à l'information, le droit d'accès, de rectification, de limitation ou d'effacement, sont exercés conformément aux règles nationales relatives à la procédure judiciaire.

L'al. 1 dispose que les droits des personnes concernées dans le cadre de procédures pendantes devant des tribunaux fédéraux ou dans le cadre de procédures régies par le CPP ou par l'EIMP sont régis par le droit de procédure applicable. Il s'agit d'une norme de coordination entre la LPDS et le droit de procédure. Le but est d'éviter un conflit de normes. L'al. 1 fixe le principe selon lequel seul le droit de procédure applicable détermine les droits des personnes concernées. En d'autres termes, cela signifie par exemple que les parties à une procédure ne peuvent pas faire valoir le droit d'accès (art. 17 LPDS) afin de consulter un dossier pénal ou d'entraide judiciaire, ni faire valoir les prétentions découlant de l'art. 19 LPDS tels que les droits d'effacement ou de rectification des données. Tant que la procédure est pendante, ces droits sont exclusivement régis par le droit de procédure applicable.

Une fois la procédure close, la LPDS, et à titre subsidiaire la LPD, s'appliquent. Ce régime reste inchangé par rapport au droit en vigueur (art. 2, al. 2, let. c, LPD *a contrario*). Il correspond également à la solution prévue à l'art. 99, al. 1, CPP: après la clôture de la procédure pénale, le traitement des données, la procédure et les voies de droit sont régis par les dispositions fédérales et cantonales sur la protection des données.

Al. 2: application de la LPD à titre subsidiaire

Cette disposition règle l'articulation entre la LPDS, la LPD et les dispositions spéciales des lois sectorielles. Elle consacre le principe selon lequel la protection des données personnelles dans le cadre de Schengen est en principe régie par la LPDS et les dispositions spéciales de protection des données des lois sectorielles, y compris celles introduites dans le CP, le CPP, l'EIMP et la LSIP. A titre d'exemple, on peut citer, pour le domaine d'entraide judiciaire, les nouvelles dispositions prévues aux art. 11*b* et suivants EIMP et d'autres dispositions en vigueur tels que l'art. 52 relatif au droit d'être entendu de la personne poursuivie ou encore le droit des ayants droit de participer à une procédure d'entraide judiciaire et de consulter le dossier (art. 80*b* EIMP). Ces dispositions constituent une réglementation suffisante au regard des exigences de la directive (UE) 2016/680 en matière de transparence des traitements de données personnelles.

A défaut de dispositions de protection des données prévues par la LPDS ou par d'autres lois fédérales spéciales, les dispositions générales de protection des données de la LPD s'appli-

[21] RS **235.1**

quent, par exemple le but (art. 1), certaines définitions de l'art. 3 LPD, la sécurité des données (art. 7), le registre des fichiers (art. 11a), le devoir d'informer lors de la collecte de données personnelles (art. 18*a* et 18*b*) la proposition des documents aux archives fédérales (art. 21), etc.

Art. 3 Définitions

En sus des définitions de l'art. 3 LPD, la LPDS définit de nouvelles notions que l'on trouve aux art. 3 et 10 de la directive (UE) 2016/680.

Al. 1, let. a: données personnelles sensibles

La let. a définit la liste des données sensibles.

Contrairement à la définition prévue à l'art. 3, let. c, ch. 1, LPD, la LPDS ne qualifie pas les données sur les opinions ou activités syndicales en tant que données sensibles. Le Parlement a en effet considéré que cette catégorie de données est comprise dans celle relative aux données sur les opinions ou les activités politiques et qu'il est donc inutile de les mentionner à l'art. 3, let. a, ch. 1, LPDS. Cette modification n'a aucune portée matérielle comme l'indiquent clairement les travaux préparatoires[22].

Le ch. 2 vise non seulement les données sur l'origine raciale, mais aussi celles sur l'origine ethnique, comme le prévoit la directive (UE) 2016/680 (art. 10). Le recours à la notion d'« origine raciale » n'implique en aucune façon l'adhésion à des théories tendant à établir l'existence de races humaines distinctes.

La notion de « données sensibles » est par ailleurs élargie aux données génétiques (ch. 3) et aux données biométriques identifiant une personne physique de façon unique (ch. 4). Cette modification transpose les exigences de la directive (UE) 2016/680 (art. 10).

Les données génétiques sont les informations relatives au patrimoine génétique d'une personne obtenues par une analyse génétique, y compris le profil d'ADN (art. 3, let. l, de la loi fédérale du 8 octobre 2014 sur l'analyse génétique humaine [LAGH][23]).

Par données biométriques, on entend ici les données personnelles résultant d'un traitement technique spécifique et relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment son identification unique. Il s'agit par exemple des empreintes digitales, des images faciales, de l'iris, ou encore de la voix. Ces données doivent impérativement résulter d'un traitement technique spécifique qui permet l'identification ou l'authentification unique d'un individu. Tel ne sera en principe pas le cas, par exemple, de simples photographies.

Al. 1, let. b: profilage

La LPDS introduit la notion de profilage.

Cette définition correspond à celle prévue à l'art. 3, ch. 4, de la directive (UE) 2016/680. Le Parlement a décidé de s'écarter de la définition proposée par le Conseil fédéral dans son projet de révision totale de la LPD et de s'aligner sur le texte européen. Selon cette définition, on entend par « profilage » toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne. Le recours à des algorithmes est possible mais non constitutif du profilage. En revanche, un

[22] BO 2018 N 977 et BO 2018 E 620

[23] RS **810.12**

traitement automatisé des données est indispensable. La simple accumulation de données n'est pas assimilée au profilage.

En tant que traitement susceptible de porter gravement atteinte aux droits fondamentaux des personnes concernées (art. 36 Cst.), le profilage doit reposer sur une base légale au sens formel (voir le commentaire de l'art. 6, al. 2, let. c, LPDS).

Al. 1, let. c: violation de la sécurité des données

La LPDS définit la notion de « violation de la sécurité des données ». Est considérée comme telle toute violation de la sécurité entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données, et ce indépendamment de la question de savoir si la violation est intentionnelle ou non, licite ou illicite. Le terme est lié à l'art. 7 LPD, selon lequel les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. La notion correspond à celle de l'art. 3, ch. 11, de la directive (UE) 2016/680.

Ce qui compte, c'est que l'événement en question ait eu lieu. Peu importe que la divulgation ou un accès non autorisés se soient effectivement produits ou aient simplement été rendus possibles. En effet, lorsqu'un support de données a été perdu, il est souvent difficile de prouver que les données qu'il contenait ont été vues ou utilisées par des personnes non autorisées. C'est pourquoi la perte de cet objet constitue en elle-même une violation de la sécurité des données. Ce sont plutôt l'ampleur et la signification d'une telle violation qui sont déterminantes pour les mesures à prendre, en particulier pour l'estimation du risque conformément à l'art .15, al. 1, LPDS.

Al. 1, let. d: décision individuelle automatisée

Pour mettre en œuvre les exigences de l'art. 11 de la directive (UE) 2016/680, la LPDS introduit la notion de « décision individuelle automatisée ». Une décision est considérée comme telle lorsqu'une exploitation de données a lieu sans intervention humaine et qu'il en résulte une décision, ou un jugement, à l'égard de la personne concernée. Le fait que la décision soit au final communiquée par une personne physique, à savoir un employé de l'organe fédéral compétent, ne change rien à son caractère automatisé, car cette personne n'a pas d'influence sur le processus de décision. La question déterminante est ainsi celle de savoir dans quelle mesure une personne physique peut faire un examen de la situation et se baser sur ses considérations pour rendre une décision finale. Cette décision doit cependant présenter un certain degré de complexité. Pour le surplus, il convient de se référer au commentaire de l'art. 11 LPDS.

Al. 1, let. e: sous-traitant

Il s'agit de la personne privée ou de l'organe fédéral qui traite des données pour le compte de l'organe fédéral. Cette notion reprend celle de la directive (UE) 2016/680 (art. 3, ch. 9).

Le rapport juridique liant l'organe fédéral et le sous-traitant peut être de nature diverse. Il peut s'agir d'un contrat ou de la délégation d'une tâche publique impliquant le traitement de données personnelles. Le sous-traitant cesse d'être un tiers à compter du moment où il débute ses activités pour le compte de l'organe fédéral.

Art. 4 Principes

Al. 1 et 2

Les al. 1 et 2 fixent les principes de licéité, de bonne foi et de proportionnalité. Ils correspondent aux règles prévues à l'art. 4, al. 1 et 2, LPD. Pour éviter de régler les principaux généraux de protection des données dans deux lois différentes (LPD et LPDS), ceux-ci doivent être regroupés dans la LPDS. La sécurité du droit est ainsi mieux garantie.

Al. 3: finalité et reconnaissabilité

L'al. 3 regroupe les principes de finalité et de reconnaissabilité contenus aux al. 3 et 4 de l'art. 4 LPD. La nouvelle formulation n'implique pas de changements matériels par rapport au droit en vigueur: tant la collecte des données que les finalités du traitement doivent être reconnaissables pour la personne concernée. On considère que tel est le cas lorsque ces traitements sont prévus par la loi.

L'al. 3 mentionne encore que les données doivent être traitées ultérieurement de manière compatible avec les finalités initiales.

Tel est notamment le cas lorsque la modification du but initial est prévue par la loi ou requise par un changement législatif. L'art. 96, al. 1, CPP est également un cas d'application. Cette norme prescrit que l'autorité pénale peut divulguer des données personnelles relevant d'une procédure pénale pendante pour permettre leur utilisation dans le cadre d'une autre procédure pendante lorsqu'il y a lieu de présumer que ces données contribueront dans une notable mesure à l'élucidation des faits.

Dans le domaine de la coopération judiciaire internationale en matière pénale, le principe de finalité correspond au principe de spécialité: les données transmises doivent être utilisées uniquement dans la procédure pénale à l'origine de la demande. Toute autre utilisation par l'autorité compétente de l'Etat requérant est soumise à l'autorisation de l'Etat requis.

Al. 4: durée de conservation des données personnelles

Selon l'al. 4, les données doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement. Cette exigence correspond à ce que prévoit la directive (UE) 2016/680 (art. 4, par. 1, let. e). Elle découle implicitement du principe général de proportionnalité énoncé à l'art. 4, al. 2 LPDS. Il est toutefois important, compte tenu des évolutions technologiques et des capacités presque illimitées de stockage, de la mentionner expressément. Dans le secteur public, les délais de conservation sont en principe fixés par le législateur.

Al. 5: exactitude

L'al. 5 reprend le principe de l'exactitude des données figurant à l'art. 5 LPD. Le terme de « correctes » est remplacé dans le texte français par celui d'« exactes »; en allemand et en italien, la terminologie est déjà celle-ci.

Le texte prévoit que celui qui traite des données personnelles doit s'assurer qu'elles sont exactes. Il prend toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Les données qui ne peuvent être rectifiées ou complétées doivent être effacées ou détruites. L'étendue du devoir d'exactitude doit être déterminée de cas en cas. Elle dépend notamment de la finalité du traitement ainsi que de son ampleur, et du type de données traitées. Le devoir d'exactitude peut impliquer selon les cas de tenir les données à jour.

Certaines obligations légales peuvent s'opposer à la rectification, à l'effacement, ou à la mise à jour des données[24].

Contrairement à la LPD, la LPDS ne définit pas la notion de « consentement ». En effet, en vertu de la directive (UE) 2016/680, les traitements de données personnelles tombant dans son champ d'application et qui se basent uniquement sur le consentement de la personne concernée sont illicites[25]. Le consentement de la personne concernée peut être une modalité du traitement des données mais non sa base juridique. Selon l'exemple donné au considérant 35 de la directive (UE) 2016/680, les Etats Schengen peuvent prévoir *par la loi* que la personne concernée peut consentir au traitement de données personnelles la concernant, par exemple pour des tests ADN dans des enquêtes pénales. L'art. 80*c* EIMP est un autre cas d'application. Cette disposition règle l'exécution simplifiée de l'entraide judiciaire et prescrit à l'al. 1 que les détenteurs de documents ou de renseignements peuvent accepter que ces informations soient remises à l'Etat requérant.

Art. 5 Protection des données dès la conception et par défaut

L'art. 5 LPDS instaure l'obligation de protéger les données dès la conception et par défaut. Cette obligation étant étroitement liée aux principes de la protection des données, elle est introduite dans les dispositions générales de la loi. Cette disposition met en œuvre les exigences de l'art. 20 de la directive (UE) 2016/680.

La protection de la sphère privée des personnes concernées à l'égard du traitement de leurs données exige l'adoption de mesures techniques et organisationnelles appropriées (art. 7 LPD et art. 8, 10 et 20 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données [OLPD][26]). La mise en œuvre de telles mesures ne doit pas dépendre uniquement de considérations économiques. Afin de pouvoir démontrer qu'il respecte les prescriptions de protection des données, l'organe fédéral doit adopter les mesures internes nécessaires et mettre en œuvre les mesures qui respectent en particulier la protection des données dès la conception et par défaut. Lorsque l'organe fédéral a établi une analyse d'impact de la protection des données conformément à l'art. 13 LPDS, les résultats doivent être pris en compte pour l'élaboration de ces mesures.

Al. 1: protection des données dès la conception

L'al. 1 impose à l'organe fédéral de concevoir dès l'origine le traitement de données de telle manière qu'il respecte les prescriptions relatives à la protection des données. La nouvelle obligation repose sur le principe de la technologie au service de la protection des données personnelles (*privacy by design*). Le recours à des solutions techniques pour garantir la protection des données s'appuie sur l'idée que la technologie et le droit se complètent. Ainsi, des solutions techniques qui rendent impossible une violation de la protection des données ou qui en réduisent la probabilité rendent les règles juridiques moins nécessaires. Par ailleurs, ces technologies sont indispensables pour mettre en œuvre les réglementations de protection des données. L'ampleur des traitements de données personnelles a augmenté de manière importante. Les technologies permettent de plus en plus de traiter des données dans des domaines telles que la prévention, l'élucidation ou la poursuite d'infractions pénales qu'il faut traiter dans le respect des dispositions légales. Or cela est impossible sans des solutions techniques adaptées. La protection technique des données personnelles ne s'appuie pas sur une technologie précise; elle passe plutôt par la mise en place de règles techniques et organisationnelles conformes aux principes définis à l'art. 4 LPDS. En d'autres

---

[24] Comme le devoir de conserver les données intactes, prévu par exemple à l'art. 7 de la loi fédérale du 10 octobre 1997 sur le blanchiment d'argent (RS **955.0**).

[25] Voir le considérant 35 de la directive (UE) 2016/680.

[26] RS **235.11**

termes, les exigences légales auxquelles doit satisfaire un traitement conforme à la protection des données sont déjà intégrées dans le système, de manière à rendre impossible une violation de la protection des données ou d'en réduire la probabilité. Il s'agit par exemple de la fixation d'échéances régulières pour l'effacement ou l'anonymisation systématique des données personnelles. Un principe significatif pour la protection des données au plan technique est celui de la minimisation des données. Selon ce dernier, il faut fixer avant même le début d'un traitement ses modalités, de manière à ce que le moins de données possible soient traitées, et de façon à ce qu'elles soient conservées le moins longtemps possible.

Cette disposition n'a pratiquement pas de portée pour les organes fédéraux. En effet, ces derniers sont aujourd'hui déjà tenus d'annoncer à leurs conseillers à la protection des données, ou au Préposé fédéral à la protection des données et à la transparence (« préposé »), tous les projets impliquant un traitement automatisé de données. Les exigences de protection des données sont ainsi déjà prises en compte au niveau de la conception des traitements (voir l'art. 20 OLPD).

Al. 2: caractère approprié des mesures

L'al. 2 précise les exigences auxquelles doivent satisfaire les mesures visées à l'al. 1. Ces mesures doivent être appropriées au regard notamment de l'état de la technique, du type de traitement, de son étendue et du degré de probabilité et de gravité du risque que le traitement des données en question présente pour les droits fondamentaux des personnes concernées.

La norme matérialise l'approche fondée sur les risques telle qu'elle est consacrée par le projet de loi du Conseil fédéral du 15 septembre 2017[27]. Il faut établir un rapport entre le risque induit par le traitement et les moyens techniques permettant de le réduire. Plus le risque est élevé, plus sa survenue est probable, et plus le traitement de données est important, plus les exigences auxquelles doivent répondre les mesures techniques pour être considérées comme appropriées au sens de cette disposition seront élevées.

Al. 3: protection des données par défaut

Selon l'al. 3, l'organe fédéral est tenu, par le biais de préréglages appropriés, de garantir que le traitement soit limité au minimum requis par la finalité poursuivie (*privacy by default*). Dans le contexte de la protection des données, cela signifie que le processus de traitement doit être préprogrammé de manière à garantir autant que possible la protection des données. Le lien avec la protection des données dès la conception est étroit. En effet, ces réglages prédéfinis s'inscrivent souvent dans un système entier respectueux de la protection des données.

Art. 6 Bases légales relatives au traitement de données personnelles

L'art. 6 LPDS règle le niveau de la base légale pour le traitement de données personnelles. Il reprend en partie l'art. 17 LPD tout en introduisant d'autres types de traitements qui nécessitent une base légale au sens formel conformément aux exigences de la directive (UE) 2016/680.

Al. 1: principe

Cette disposition reprend le principe qui figure à l'art. 17, al. 1, LPD, selon lequel les organes fédéraux ne sont en droit de traiter des données personnelles que s'il existe une base légale, sous réserve de certaines exceptions.

[27] FF 2017 6565 6593

Al. 2: base légale au sens formel

Les let. a et b de l'al. 2 prescrivent, comme c'est déjà le cas aujourd'hui, que les traitements de données sensibles et de profils de la personnalité doivent reposer sur une base légale au sens formel.

En vertu de l'al. 2, let. c, les organes fédéraux ne sont en droit d'effectuer des profilages au sens de l'art. 3, al. 1, let. b, LPDS que si une base légale au sens formel le prévoit. En raison du risque d'atteinte aux droits fondamentaux des personnes concernées, l'exigence du niveau de la base légale pour le profilage doit être la même que celle pour le traitement de données sensibles et de profils de la personnalité.

L'al. 2, let. d, prescrit qu'une base légale au sens formel est exigée lorsque le mode du traitement est susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée. Il ne s'agit pas d'une exigence véritablement nouvelle puisque l'art. 36, al. 1, Cst. prescrit déjà que toute restriction grave d'un droit fondamental doit être fondée sur une base légale prévue par une loi au sens formel.

A titre d'exemple, les décisions individuelles automatisées au sens de l'art. 3, al. 1, let. d, LPDS constituent des modes de traitements susceptibles de porter une atteinte grave aux droits fondamentaux des personnes concernées. Lorsque ce n'est pas le cas toutefois, une base légale au sens matériel est suffisante. En principe, lorsque la décision individuelle automatisée se fonde sur un traitement de données sensibles, une base légale au sens formel doit être prévue. Les exigences de l'art. 11 de la directive (UE) 2016/680 sont ainsi respectées.

Al. 3: dérogations

Cette disposition prévoit une dérogation à l'exigence d'une base légale (al. 1 et 2) si l'une des conditions prévues aux let. a et b est réalisée.

En vertu de la let. a, les organes fédéraux peuvent traiter des données personnelles si le traitement est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers. Cette exception est nouvelle par rapport l'art. 17, al. 2, LPD. Elle correspond à l'art. 10, let. b, de la directive (UE) 2016/680.

En vertu de la let. b, les organes fédéraux peuvent également traiter des données si la personne concernée a rendu ses données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement. Cette disposition correspond en partie à l'exception prévue à l'art. 17, al. 2, let. c, LPD.

Contrairement à la LPD, la LPDS ne prévoit pas le « consentement » comme exception à l'exigence d'une base légale. En effet, en vertu de la directive (UE) 2016/680, les traitements de données personnelles tombant dans son champ d'application et qui se basent uniquement sur le consentement de la personne concernée sont illicites[28] (voir ci-dessus le commentaire de l'art. 4 LPDS).

Art. 7 Bases légales relatives à la communication de données personnelles

L'art. 7 LPDS reprend en partie l'art. 19 LPD.

L'al. 1 met en œuvre les art. 8 et 10 de la directive (UE) 2016/680, qui prévoient en substance qu'un traitement de données tombant dans le champ d'application de ladite directive n'est licite que s'il repose sur une base légale ou, à défaut, dans certains cas spécifiques énumérés par les dispositions susmentionnées.

[28] Voir les considérants 35 et 37 de la directive (UE) 2016/680.

Selon l'al. 2, les al. 1^bis à 4 de l'art. 19 LPD s'appliquent pour le surplus.

Art. 8 Communication de données personnelles à l'étranger

L'al. 1 met en œuvre l'art. 9, par. 3 et 4, de la directive (UE) 2016/680. Il instaure une égalité de traitement entre les autorités des Etats Schengen et les autorités pénales suisses en matière de protection des données[29]. Cette disposition correspond à la solution retenue par le législateur fédéral à l'art. 6 LEIS. Les communications de données à des autorités d'un Etat Schengen ou à une autorité nationale sont soumises aux mêmes conditions de protection des données. L'adoption de nouvelles restrictions légales reste possible, pour autant que le principe d'égalité soit respecté.

Quant à l'al. 2, il prescrit que la communication de données personnelles à un Etat tiers ou à un organisme international est régie par les dispositions spéciales des lois fédérales applicables, à savoir par les art. 349*c* à 349*e* et 335*a*, al. 4, CP en matière de coopération policière, et par les art. 11*f* à 11*g* EIMP en ce qui concerne l'entraide judiciaire.

Art. 9 Organe fédéral responsable et contrôle

Par rapport à l'art. 16 LPD, l'art. 9, al. 2, LPDS subit quelques modifications à des fins de mise en œuvre de l'art. 21 de la directive (UE) 2016/680.

L'al. 1 correspond à l'art. 16, al. 1, LPD.

L'al. 2 supprime les termes « de manière spécifique » de l'art. 16, al. 2, LPD, pour des motifs rédactionnels. Il prévoit par ailleurs une obligation – et non plus seulement une faculté – pour le Conseil fédéral de régler les procédures de contrôle et les responsabilités en matière de protection des données lorsqu'un organe fédéral traite des données conjointement avec d'autres autorités ou des personnes privées.

Art. 10 Sous-traitance

L'art. 10 LPDS met en œuvre les exigences de l'art. 22 de la directive (UE) 2016/680. L'al. 1 relatif à la sous-traitance d'un traitement de données personnelles à un sous-traitant renvoie pour l'essentiel à l'art. 10*a* LPD (concernant la définition légale voir l'art. 3, al. 1, let. e, LPDS).

L'organe fédéral responsable a, comme dans le droit en vigueur, un devoir de diligence relatif au travail accompli par le sous-traitant. Il doit s'assurer de manière active que le sous-traitant respecte le droit de la protection des données dans la même mesure que lui. Cela concerne principalement les principes généraux de protection des données tels que l'obligation de détruire ou d'anonymiser les données personnelles dès qu'elles ne sont plus nécessaires au regard des finalités du traitement (art. 4, al. 4, LPDS) ainsi que les règles sur la sécurité qui sont expressément mentionnées à l'art. 10a, al. 2, LPD. L'organe fédéral doit, par analogie à l'art. 55 CO[30], mettre tout en œuvre pour éviter une éventuelle violation des dispositions légales de protection des données. Il doit ainsi veiller à choisir soigneusement son mandataire, à lui donner les instructions adéquates et à exercer la surveillance nécessaire. Enfin, le sous-traitant a l'obligation de tenir un registre des activités de traitement comme le prévoit l'art. 12 LPDS.

L'art. 10, al. 2, LPDS est nouveau par rapport à la LPD et prévoit que le sous-traitant ne peut lui-même sous-traiter un traitement qu'avec l'autorisation écrite préalable de l'organe fédéral. Il s'agit là d'une exigence de la directive (UE) 2016/680 (art. 22, par. 2). L'autorisation peut

[29] Voir le considérant 26 de la directive (UE) 2016/680.

[30] RS **220**

être spécifique ou générale. Dans cette seconde hypothèse, le sous-traitant informe l'organe fédéral de tout changement (ajout ou remplacement d'autres sous-traitants) lui permettant ainsi, le cas échéant, d'émettre des objections.

Un sous-traitant ne peut effectuer que les traitements que l'organe fédéral serait en droit d'effectuer lui-même (voir l'art. 10*a*, al. 1, let. a, LPD). Le LPDS s'applique par conséquent également au sous-traitant. Les pouvoirs de surveillance du préposé vis-à-vis du sous-traitant sont régis par l'art. 22 ss LPDS (et non par l'art. 27 LPD).

2.3 Obligations des organes fédéraux et des sous-traitants

Art. 11 Décision individuelle automatisée

Cette disposition met en œuvre l'art. 11 de la directive (UE) 2016/680. La notion de « décision individuelle automatisée » est définie à l'art. 3, al. 1, let. d, LPDS. Selon cette définition, cette notion vise toute décision prise exclusivement sur la base d'un traitement de données personnelles automatisé, y compris le profilage, et qui a des effets juridiques sur la personne concernée ou qui l'affecte de manière significative.

Al. 1: information de la personne concernée

Selon cet alinéa, l'organe fédéral informe la personne concernée de l'existence d'une décision individuelle automatisée. Il doit lui indiquer spécifiquement que la décision a été prise sans intervention humaine. Cette exigence est nécessaire pour que la personne concernée puisse exercer ses droits selon l'al. 2.

Le traitement de données personnelles automatisé sur lequel se base la décision peut être un profilage (art. 3, al. 1, let. b LPDS). A ce propos, l'art. 11 par. 3 de la directive (UE) 2016/680 prescrit que tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'art. 10 de la directive (soit en droit fédéral les données sensibles) est interdit conformément au droit de l'UE. Cette exigence correspond à la protection contre l'arbitraire garantie par l'art. 9 de la Constitution fédérale.

Il n'est pas nécessaire que la personne concernée soit informée de chaque décision individuelle automatisée, mais seulement lorsque la décision a pour elle des effets juridiques ou l'affecte de manière significative (art. 3, al. 1, let. d, LPDS).

La décision produit des effets juridiques lorsqu'elle a des conséquences directes et prévues par la loi pour la personne concernée. Il peut s'agir par exemple de mesures de sécurité ou de surveillance plus sévères[31].

On peut supposer que la personne concernée est affectée de manière significative lorsqu'elle est durablement entravée sur le plan personnel. Une simple nuisance ne suffit pas. Tout dépend des circonstances concrètes. Il faut en particulier tenir compte de l'importance du bien affecté pour la personne concernée, de la durée des effets de la décision et de l'existence ou non d'une solution de remplacement. Une décision pourrait par exemple affecter la personne concernée de manière significative si elle l'empêche de voyager en avion parce qu'elle figure sur une liste noire[32].

---

[31] Voir le document de travail « Opinion on some key issues of the Law Enforcement Directive (EU) 2016/680) » du 29 novembre 2017 du Groupe de travail Article 29 sur la protection des données, p. 14. Le groupe de travail est un organe consultatif indépendant de la Commission européenne chargé des questions de protection des données.

[32] Voir le document de travail « Opinion on some key issues of the Law Enforcement Directive (EU) 2016/680) » du 29 novembre 2017 du Groupe de travail Article 29 sur la protection des données, p. 14.

Al. 2: droit de faire valoir son point de vue

Selon l'al. 2, l'organe fédéral doit donner à la personne concernée, si elle le demande, la possibilité de faire valoir son point de vue sur le résultat de la décision, et même de demander comment la décision a été prise. Elle peut exiger que la procédure appliquée lui soit communiquée et que la décision soit revue par une personne physique. Le but est entre autres d'éviter que le traitement de données soit effectué sur la base de données incomplètes, dépassées ou non pertinentes. Cette règle est également dans l'intérêt de l'organe fédéral, pour lequel une décision individuelle automatisée erronée peut aussi avoir des conséquences négatives. La loi ne précise pas à quel moment la personne concernée doit être informée ni quand elle a la possibilité d'exposer son point de vue. Cela peut donc se faire avant ou après la décision. Il est ainsi notamment possible de lui notifier une décision individuelle automatisée – qui sera désignée comme telle – et de l'entendre dans le cadre de l'exercice du droit d'être entendu.

Al. 3: exception

L'al. 3 prévoit que l'al. 2 ne s'applique pas lorsque la personne dispose d'une voie de recours. La personne concernée fera valoir son point de vue et fera examiner la décision par une personne physique dans ce cadre. En d'autres termes, les droits garantis par l'art. 11, al. 2, LPDS le sont déjà par les voies de droit usuelles.

Art. 12 Registre des activités de traitement

Cette disposition met en œuvre l'art. 24 de la directive (UE) 2016/680.

La tenue d'un registre des activités de traitement incombe, selon l'al. 1, aux organes fédéraux et aux sous-traitants.

L'al. 2 précise les indications minimales que doit contenir le registre, à commencer par le nom de l'organe fédéral responsable (let. a) et la finalité du traitement (let. b). Le registre doit aussi donner une description des catégories des personnes concernées et des catégories des données personnelles traitées (let. c). Les catégories des données personnelles traitées désignent la nature des données (données sensibles, par ex.). Le registre doit également indiquer les catégories des destinataires auxquels les données sont susceptibles d'être communiquées (let. d). Selon la let. e, le registre doit contenir le délai de conservation des données personnelles. Ce délai étant lié, conformément à l'art. 4, al. 4, LPDS, aux finalités du traitement, il n'est pas toujours possible de l'établir avec précision. S'il n'est pas possible de fournir une indication précise, le registre doit au moins indiquer les critères selon lesquels ce délai sera fixé. Selon la let. f, le registre doit contenir, si possible, une description générale des mesures visant à garantir la sécurité des données selon l'art. 7 LPD. Le but de cette description est de faire apparaître d'éventuels manquements dans les mesures de sécurité. La mention « dans la mesure du possible » indique que cette obligation ne s'applique que si les mesures peuvent être définies de manière suffisamment concrète. Enfin, le registre doit indiquer le nom de l'Etat tiers ou de l'organisme international auquel des données personnelles sont communiquées ainsi que les garanties de protection des données personnelles prévues. Les communications de données personnelles à un Etat Schengen tombent sous le coup de la let. d. Comme la liste de l'al. 2 n'est pas exhaustive, les registres d'activité de traitement doivent, selon les circonstances, contenir d'autres indications comme le profilage (art. 24, par. 1, let. e, de la directive [UE] 2016/680).

L'énumération de l'al. 2 montre clairement que le registre est un descriptif général des activités de traitement, qui permet de déduire la nature et l'ampleur de celles-ci. Il fournit, par écrit, les indications importantes relatives à tous les traitements de données de l'organe fédéral responsable ou d'un sous-traitant. Il permet donc de savoir de manière assez précise si un traitement de données est, en principe, conforme ou non à la protection des données.

L'al. 3 contient une liste abrégée des indications minimales devant figurer sur le registre du sous-traitant, dont les catégories de traitements effectués pour le compte de l'organe fédéral responsable. Ce registre contient donc aussi le nom de l'autorité pour laquelle le sous-traitant travaille.

L'art. 12 LPDS n'implique pas de changement pour les organes fédéraux puisque ceux-ci ont déjà l'obligation d'établir un règlement de traitement (art. 21 OLPD).

Art. 13 Analyse *d'impact* relative à la protection des données personnelles

L'art. 13 LPDS instaure une obligation de procéder à une analyse d'impact relative à la protection des données personnelles. Cette disposition concrétise les exigences posées aux art. 27 ss de la directive (UE) 2016/680. Comme le relève le considérant 58 de la directive européenne, les analyses d'impact portent sur des systèmes de traitement de données personnelles et non sur des cas individuels.

La définition et le rôle de l'analyse d'impact résultent de l'al. 13, al. 3, LPDS. Il s'agit d'un instrument destiné à identifier et à évaluer les risques que certains traitements de données personnelles pourraient entraîner pour les personnes concernées. Le cas échéant, cette analyse doit servir à définir des mesures pour faire face à ces risques.

L'art. 13 a une portée limitée pour les organes fédéraux. En effet, ceux-ci doivent aujourd'hui déjà annoncer les projets impliquant des traitements automatisés de données aux conseillers à la protection des données ou, à défaut, au préposé (art. 20, al. 2, OLPD). Le processus de la méthode de gestion de projets Hermès devrait largement correspondre aux exigences de l'analyse d'impact.

Al. 1 et 2: motifs justifiant la réalisation d'une analyse d'impact

L'al. 1 prévoit que l'organe fédéral procède à une analyse d'impact lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour les droits fondamentaux des personnes concernées[33]. L'autorité est donc tenue de faire un pronostic des conséquences que les traitements en question peuvent avoir. Sont déterminants, notamment, la nature et l'ampleur de l'impact du traitement sur les droits fondamentaux des personnes concernées.

Pour évaluer le risque, l'organe fédéral doit faire un lien entre, d'une part, les traitements envisagés et, d'autre part, les droits des personnes concernées à la protection de leur sphère privée. Un risque élevé pour les droits fondamentaux des personnes concernées peut résulter, par exemple, de la nature ou du contenu des données à traiter (par ex. données sensibles ou profils de la personnalité), ou de la nature ou de la finalité du système de traitement envisagé (par ex. profilage).

L'al. 2 précise que l'existence d'un risque élevé dépend, en particulier lors de l'utilisation de nouvelles technologies, de la nature, de l'étendue, des circonstances et de la finalité des traitements. Plus les traitements sont étendus, plus les données sont sensibles et plus la finalité est vaste, plus il y a lieu de conclure à un risque élevé. L'al. 2 mentionne deux exemples dans lesquels un tel risque existe: selon la let. a, c'est le cas lorsque le système de traitement concerne un grand volume de données sensibles ou lorsqu'il s'agit d'établir des profils de la personnalité à grande échelle. La let. b dispose qu'un risque élevé existe aussi en cas de profilage. Tel peut être également le cas lorsque des décisions sont prises exclusivement sur la base de traitements de données personnelles automatisés, y compris en cas de profilage, et que ces décisions ont des effets juridiques sur les personnes concernées ou l'affectent de manière notable. Il ne faut pas perdre de vue en effet que ce type de décisions

[33] Voir les Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is « likely to result in a high risk » for the purposes of Regulation 2016/679, document de travail du 4 avril 2017 du Groupe Article 29, pp. 7 ss en particulier.

peuvent, selon le cas, avoir des répercussions non négligeables pour les individus. Une analyse d'impact est également nécessaire dans de telles situations.

La 2e phrase de l'al. 1 autorise l'organe fédéral à effectuer une analyse d'impact commune s'il envisage d'effectuer plusieurs opérations de traitement semblables. Sont visés en particulier les traitements poursuivant un objectif supérieur commun. En pareil cas, il n'est pas nécessaire d'examiner individuellement chacune des étapes prévues dans un système de traitement. L'analyse d'impact peut porter sur la plateforme dans son ensemble.

Al. 3: contenu de l'analyse d'impact relative à la protection des données personnelles

Selon l'al. 3, l'analyse d'impact relative à la protection des données doit tout d'abord exposer les traitements envisagés. Il faut ainsi présenter les différents processus (par ex. la technologie employée), la finalité du traitement ou la durée de conservation des données personnelles. Par ailleurs, l'analyse d'impact doit montrer quels risques les traitements impliquent pour les droits fondamentaux des personnes concernées. Il s'agit ici d'un approfondissement de l'évaluation des risques qui doit déjà être faite en amont, lors de l'examen de la nécessité de procéder à une analyse d'impact. Il convient ainsi de présenter la nature du risque élevé qu'engendrent les traitements envisagés et les moyens de l'évaluer. Enfin, l'analyse d'impact doit expliquer les mesures prévues pour faire face à ce risque. Il s'agira souvent de mettre en œuvre les principes de l'art. 4 LPDS, ainsi que les principes de protection dès la conception et par défaut (*privacy by design/by default*; art. 5 LPDS).

Art. 14 Consultation du Préposé fédéral à la protection des données et à la transparence

Al. 1: obligation de consulter le préposé

Aux termes de l'al. 1, l'organe fédéral doit obtenir une prise de position du préposé préalablement au traitement s'il ressort de l'analyse d'impact que le traitement envisagé présenterait un risque élevé pour les droits fondamentaux de la personne concernée si aucune mesure n'était prise. Cette consultation préalable correspond aux exigences de l'art. 28 de la directive (UE) 2016/680.

Al. 2 et 3: objections du préposé

Le préposé a deux mois suivant la réception de la communication pour faire part à l'organe fédéral de ses objections concernant le traitement envisagé. Dans des cas particulièrement compliqués, ce délai peut être prolongé d'un mois. Si l'autorité ne reçoit pas de nouvelles du préposé dans le délai de deux mois, elle peut partir du principe que le préposé n'a pas d'objections contre le traitement envisagé.

Lorsqu'il est informé du résultat d'une analyse d'impact, le préposé vérifie si les mesures proposées sont suffisantes pour protéger les droits fondamentaux de la personne concernée. S'il arrive à la conclusion que le traitement contreviendrait, dans la forme envisagée, aux dispositions de la protection des données, il conseille l'organe fédéral sur les mesures appropriées à prendre.

Le préposé n'en reste pas moins libre d'ouvrir une enquête ultérieurement si les conditions de l'art. 22 LPDS sont remplies, en particulier s'il apparaît que les risques n'ont pas été correctement évalués dans le cadre de l'analyse d'impact et que, par conséquent, les mesures définies ratent leur cible ou sont insuffisantes.

Art. 15 Annonce des violations de la sécurité des données

L'art. 15 LPDS instaure l'obligation d'annoncer toute violation de la sécurité des données personnelles. Cette disposition concrétise les exigences fixées aux art. 30 s. de la directive (UE) 2016/680.

Al. 1: notion et fondements

L'al. 1 dispose que l'organe fédéral annonce au préposé dans les meilleurs délais toute violation de la sécurité des données entraînant vraisemblablement un risque élevé pour les droits fondamentaux de la personne concernée. Cette disposition diffère légèrement de l'art. 30 par. 1 de la directive (UE) 2016/680 qui prévoit que le responsable du traitement doit notifier à l'autorité de contrôle un cas de violation dans les meilleurs délais et, si possible, dans un délai de 72 heures au plus tard après en avoir pris connaissance, à moins qu'il soit peu probable que la violation en question n'engendre des risques pour les droits et les libertés d'une personne physique.

La notion de « violation de la sécurité des données » est définie à l'art. 3, al. 1, let. c, LPDS. On entend par là toute violation de la sécurité, sans égard au fait qu'elle soit intentionnelle ou illicite, qui entraîne la perte de données personnelles, leur modification, leur effacement ou leur destruction, ou encore leur divulgation ou un accès non autorisés. La violation peut être causée par un tiers, mais son auteur peut aussi être un collaborateur qui outrepasse ses compétences ou qui fait preuve de négligence.

L'organe fédéral doit annoncer tout traitement non autorisé au préposé en premier lieu et, si les conditions de l'al. 4 sont remplies, à la personne concernée également. L'annonce doit avoir lieu dans les meilleurs délais à partir du moment où le traitement non autorisé est connu. L'autorité doit en principe agir rapidement, mais la disposition lui laisse une certaine marge d'appréciation, qui dépend en pratique de l'ampleur du risque pour la personne concernée. Plus ce risque est élevé et le nombre de personnes concernées important, plus son intervention doit être rapide. L'annonce au préposé n'est toutefois nécessaire que s'il est vraisemblable que la violation de la sécurité des données entraînera un risque élevé pour les droits fondamentaux de la personne concernée. Il s'agit d'éviter l'annonce de violations insignifiantes. L'organe fédéral doit évaluer dans tous les cas les conséquences possibles de la violation pour la personne concernée.

Al. 2: contenu de l'annonce

L'al. 2 précise les indications que l'annonce au préposé doit contenir au minimum. L'organe fédéral doit tout d'abord indiquer la nature de la violation, pour autant que cela lui soit possible. On distingue quatre types de violations: l'effacement ou la destruction de données, leur perte, leur modification ou leur communication à des tiers non autorisés. L'annonce doit aussi expliquer, dans la mesure du possible, les conséquences de la violation de la sécurité des données. Enfin, il y a lieu de préciser également les mesures prises ou envisagées pour remédier à la violation de la sécurité des données ou pour atténuer ses conséquences. L'annonce doit permettre dans tous les cas au préposé d'intervenir le plus rapidement et le plus efficacement possible.

Al. 3: annonce par le sous-traitant

La violation de la sécurité des données peut aussi se produire chez le sous-traitant, qui veille, le cas échéant, à informer l'organe fédéral dans les meilleurs délais de tout traitement non autorisé. Il revient ensuite à l'organe fédéral de procéder à une évaluation des risques et de décider si une notification au préposé et à la personne concernée s'impose.

Al. 4: information de la personne concernée

Selon l'al. 4, la personne concernée ne doit être informée que si les circonstances le requièrent ou que le préposé le demande. Il existe une marge d'appréciation assez large pour déterminer si la première condition est réalisée.

Al. 5: restrictions du devoir d'informer la personne concernée

L'al. 5 dispose que l'organe fédéral peut restreindre l'information de la personne concernée, la différer ou y renoncer dans les cas visés aux let. a à e. Les let. a et b correspondent aux motifs de restriction prévus à l'art. 9 LPD (restriction du droit d'accès). La let. d admet aussi une restriction de l'information s'il n'est pas possible de respecter le devoir d'informer ou que l'information nécessite des efforts disproportionnés. Le devoir d'informer est réputé impossible à respecter lorsque l'organe fédéral n'est pas en mesure d'identifier les personnes concernées par la violation de la sécurité des données, par exemple parce que les fichiers journaux qui permettraient une identification ne sont plus disponibles. On estime de même que l'information nécessite des efforts disproportionnés dès lors qu'il faudrait informer individuellement un grand nombre de personnes concernées et que les coûts qui en résulteraient semblent excessifs au regard du gain qu'en retireraient les personnes concernées. C'est notamment dans ces cas de figure que peut s'appliquer la let. e: cette disposition autorise l'organe fédéral à opter pour une communication publique si l'information des personnes concernées est garantie de manière équivalente. On estime que cette condition est remplie quand une annonce individuelle ne permettrait pas d'améliorer sensiblement l'information de la personne concernée. L'application de l'al. 5 doit respecter le principe de proportionnalité. Toutefois, lorsque le fait de différer ou de limiter l'information de la personne concernée ne permet pas d'éviter de porter préjudice à une enquête, une instruction ou une procédure administrative ou judiciaire, l'organe fédéral peut renoncer à informer cette dernière (al. 5, let. c)[34]. Cette exception est conforme à l'art. 31 par. 5 de la directive (UE) 2016/680 qui prescrit que la communication à la personne concernée peut être retardée, limitée ou omise, sous réserve des conditions et pour les motifs prévus à l'art. 13 par. 3 qui règle la limitation du devoir d'information du responsable du traitement lorsque la protection d'un intérêt public prépondérant l'exige, telles que la sécurité publique ou une enquête en cours.

Art. 16 Conseiller à la protection des données

Conformément à l'art. 32 de la directive (UE) 2016/680, les organes fédéraux sont tenus de nommer un conseiller à la protection des données[35]. Aujourd'hui, seuls les départements et la Chancellerie fédérale doivent désigner un conseiller à la protection des données comme le prévoit l'art. 23, al. 1, OLPD. Il est donc nécessaire d'adopter une réglementation spéciale pour les organes fédéraux tombant dans le champ d'application de la LPDS. Ceux-ci peuvent le cas échéant nommer un conseiller à la protection des données commun. L'art. 16 a en pratique une portée limitée puisque la plupart des autorités concernées ont déjà aujourd'hui un conseiller à la protection des données.

Le conseiller à la protection des données veille au respect des prescriptions de protection des données et prodigue des conseils en matière de protection des données. L'organe fédéral est cependant le seul responsable du traitement en bonne et due forme des données personnelles.

L'al. 2 fixe les conditions que doit remplir le conseiller à la protection des données. Selon la let. a, celui-ci doit avoir les connaissances professionnelles nécessaires pour exercer cette tâche, s'agissant notamment de la législation en matière de protection des données et des normes techniques relatives à la sécurité des données. Pour garantir une certaine indépendance, la let. b lui interdit en outre d'exercer des activités incompatibles avec sa mission, ce qui pourrait être le cas, par exemple, s'il exerçait des fonctions dans le domaine de la gestion des systèmes informatiques, ou s'il appartenait à un service qui traite des données person-

[34] Voir le considérant 62 de la directive (UE) 2016/680.

[35] Remarque terminologique: Contrairement au P-LPD, la version allemande du LPDS recourt, comme le droit en vigueur, à la notion de « Datenschutzverantwortlicher ». Dans le cadre de la révision totale de la LPD, il est prévu de la remplacer pour plus de clarté par celle de « Datenschutzberater ».

nelles sensibles. Rien n'interdit en revanche d'imaginer qu'un conseiller à la protection des données puisse être en même temps délégué à la sécurité de l'information.

L'al. 3 règle les tâches du conseiller à la protection des données qui correspondent en substance à celles prévues à l'art. 23, al. 1, OLPD.

2.4 Droits des personnes concernées

Art. 17 Droit d'accès

En vertu de l'al. 1, le droit d'accès de la personne concernée est régi par l'art. 8 LPD. L'art. 14 de la directive (UE) 2016/680 prévoit en outre que la personne concernée a également le droit d'obtenir des informations sur la durée de conservation des données (let. d) ainsi que sur ses droits en matière de protection des données (let. e et f). A ce jour, la LPD ne prévoit pas que la personne concernée a également un droit à ces informations. L'art. 17 LPDS complète dès lors l'art. 8 LPD. Cette nouvelle disposition a pour conséquence que l'organe fédéral doit également fournir à la personne concernée les informations nécessaires pour qu'elle puisse faire valoir ses droits, soit les prétentions prévues à l'art. 19 LPDS, ainsi que des renseignements sur la durée de conservation des données. La personne concernée peut ainsi savoir si l'organe fédéral conserve les données conformément aux principes de l'art. 4 LPDS.

L'al. 2 réserve les dispositions spéciales d'autres lois fédérales tels que le CPP, l'EIMP ou encore la LSIP.

Art. 18 Restriction du droit d'accès

Sous réserve de dispositions spéciales d'autres lois fédérales, la restriction du droit d'accès est régie par l'art. 9, al. 1 à 3, et 5, LPD. L'art. 12, par. 4, let. b, de la directive (UE) 2016/680 prescrit en outre que lorsque les demandes de la personne concernée (par exemple le droit d'accès), sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut, entre autres, refuser de donner suite à la demande[36]. Il doit dans ce cas démontrer le caractère manifestement infondé ou excessif de la requête. Ce motif de restriction n'est pas expressément prévu par la LPD. Celui-ci est dès lors introduit à l'art. 18 LPDS. Sa terminologie s'inspire de celle adoptée par exemple à l'art. 108 de la loi fédérale du 17 juin 2005 sur le Tribunal fédéral[37].

L'exception prévue à la seconde phrase de l'al. 1 doit être interprétée de manière restrictive et ce, à deux égards: d'un côté, l'organe fédéral ne doit pas conclure à la légère au caractère manifestement infondé, voire procédurier, de la demande; de l'autre, c'est à lui qu'il revient de choisir l'option la plus favorable pour la personne concernée dans le cas où la requête serait manifestement infondée ou procédurière. Dans la mesure du possible, il doit se contenter de restreindre la communication des renseignements, mais peut aussi, au besoin, la différer. Le refus de communiquer les informations devra être réservé aux situations dans lesquelles aucun doute n'est permis quant à la nature de la demande. La personne doit dans tous les cas être informée du motif de la restriction (art. 9, al. 5, LPD).

Il n'est pas nécessaire de justifier d'un intérêt ou d'un motif particulier pour invoquer le droit d'accès, la simple curiosité suffit. L'organe fédéral n'est donc pas habilité à requérir, de manière générale, une motivation. Le Tribunal fédéral a néanmoins relevé que la personne tenue de fournir les renseignements peut demander une justification lorsqu'elle estime être en présence d'une invocation abusive du droit d'accès[38]. Selon la jurisprudence fédérale, une

---

[36] Voir le considérant 40 de la directive (UE) 2016/680.

[37] RS **173.110**

[38] ATF **138** III 425, consid. 5.4 s., et **123** II 534, consid. 2e.

demande d'accès est potentiellement abusive dès lors qu'elle poursuit un but totalement étranger à la protection des données, par exemple économiser les frais liés à l'obtention de preuves ou se procurer des informations sur une éventuelle partie adverse[39]. Si l'auteur de la demande fait alors valoir un motif que l'on peut qualifier d'emblée – c'est-à-dire sans clarifications approfondies et de manière certaine – d'infondé, l'organe fédéral peut restreindre la communication. Ce n'est qu'à ces conditions que l'on peut conclure au caractère manifestement infondé du droit d'accès. En d'autres termes, il doit être manifeste que le droit d'accès a été invoqué dans un but qui ne relève aucunement de la protection des données ou qu'il vise une finalité tout autre (par ex. intention frauduleuse). S'il n'existe pas de certitude, mais seulement un doute sur la nature de la demande, on ne saurait parler d'une demande manifestement infondée.

La demande d'accès a un caractère manifestement procédurier lorsque le droit d'accès est invoqué de manière répétée sans motif valable ou que la personne adresse sa demande à l'organe fédéral dont elle sait pertinemment qu'il ne traite pas de données la concernant. Dans ce cas non plus, l'organe fédéral ne peut pas conclure à la légère à la nature procédurière de la démarche.

Art. 19 Autres prétentions et procédure

L'art. 19 accorde à la personne concernée divers droits auxquels elle peut prétendre en cas de traitement illicite de ses données. Il est fortement inspiré de l'art. 25 LPD, avec quelques modifications. Pour éviter de régler ces prétentions dans deux lois différentes (LPD et LPDS), celles-ci sont regroupées dans la LPDS, pour une plus grande sécurité du droit.

Al. 1: demande d'abstention, de suppression ou de constatation

Hormis quelques adaptations linguistiques, l'al. 1 correspond à l'art. 25, al. 1, LPD.

Al. 2: autres prétentions

Aujourd'hui, le droit pour la personne concernée d'exiger l'*effacement* de ses données découle implicitement de l'art. 25 LPD. Pour mettre en œuvre les exigences de l'art. 16, par. 2, de la directive (UE) 2016/680, ce droit est expressément fixé à l'art. 19, al. 2. L'al. 2 met en œuvre, comme l'actuel art. 25, al. 3, LPD, le droit à la *rectification* des données inscrit à l'art. 16, par. 1, de la directive (UE) 2016/680.

Par rapport à l'art. 25, al. 3, let. a, LPD, le nouvel al. 2, let. a, est modifié en ce sens que la dernière partie de la phrase concernant l'opposition à la communication à des tiers est supprimée. En effet, ce droit est expressément régi par l'art. 20 LPD[40]. Le droit de s'opposer à la communication de données personnelles en vertu de l'art. 20 LPD n'est pas lié à un traitement illicite, contrairement aux prétentions prévues à l'art. 19 LPDS.

L'al. 2, let. b, dispose que la personne concernée peut demander que l'organe fédéral publie ou communique à des tiers sa décision concernant notamment la rectification, l'effacement ou la destruction des données, l'opposition à la communication conformément à l'art. 20 LPD (s'agissant du moins des cas de communication illicite) ou la mention du caractère litigieux des données personnelles conformément à l'art. 19, al. 4, LPDS. Cette disposition correspond pour l'essentiel à l'art. 25, al. 3, let. b, LPD.

---

[39] ATF **138** III 425, consid. 5.5

[40] Voir BANGERT JAN, Kommentar zu Art. 25/25bis DSG, in: Maurer-Lambrou Urs/Blechta Gabor (éd.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3^{e} éd., Bâle 2014, n° 62 s.

Al. 3: limitation du traitement

L'al. 3 introduit une nouvelle réglementation pour mettre en œuvre l'art. 16, par. 3, de la directive (UE) 2016/680. Cette disposition prévoit qu'au lieu de procéder à l'effacement des données litigieuses, l'organe fédéral responsable procède dans certains cas à la limitation de leur traitement.

L'al. 3 introduit ainsi une mesure moins radicale que l'effacement ou la destruction des données personnelles litigieuses. Cette disposition doit être interprétée dans ce sens que le traitement reste possible, mais uniquement s'il poursuit certaines finalités. En effet, il ne s'agit pas d'exclure tout type de traitement. Comme il ressort du considérant 47 de la directive (UE) 2016/680, la limitation d'un traitement doit être comprise en ce sens que l'organe fédéral ne peut traiter les données concernées que pour les finalités qui ont empêché leur effacement. L'al. 3 prévoit quatre cas de figure.

Selon la let. a, l'organe fédéral doit limiter le traitement des données lorsque leur exactitude est contestée par la personne concernée et que leur exactitude ou inexactitude ne peut pas être établie. Dans ce cas de figure, la limitation du traitement signifie que l'organe fédéral ne peut traiter les données litigieuses que dans le but de constater leur exactitude ou leur inexactitude. Une fois l'exactitude des données établie, l'organe fédéral peut poursuivre le traitement sans autres restrictions. Si par contre les données personnelles s'avèrent inexactes, l'organe fédéral doit les effacer ou les détruire, à moins que les let. b, c ou d ne s'appliquent au cas d'espèce.

La let. b prescrit que l'organe fédéral doit limiter le traitement lorsque la protection d'intérêts prépondérants d'un tiers l'exige, par exemple lorsque l'effacement ou la destruction de certaines données pourrait empêcher une tierce personne d'exercer ses droits en justice. Cette mesure signifie que le traitement des données ne reste possible que s'il a pour but de permettre au tiers concerné d'exercer ses droits. Tout traitement poursuivant une autre finalité est exclu.

En vertu de la let. c, l'organe fédéral n'est pas tenu d'effacer ou de détruire des données litigieuses lorsqu'une telle mesure risque de porter atteinte à un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Suisse.

Enfin, la let. d dispose que l'organe fédéral n'est pas non plus tenu d'effacer ou de détruire des données lorsqu'une telle mesure risque de compromettre une enquête, une instruction ou une procédure administrative ou judiciaire. Dans ce cas de figure, l'organe fédéral peut continuer à traiter des données personnelles, mais uniquement pour les finalités qui ont empêché leur effacement, à savoir la poursuite d'une enquête, d'une instruction ou d'une procédure.

La limitation du traitement signifie que les données litigieuses doivent être marquées de telle manière qu'elles ne puissent être traitées que pour la finalité qui a empêché leur effacement ou leur destruction. Le marquage doit être clair. Une solution envisageable en pratique est de faire migrer provisoirement les données litigieuses dans un autre système. Il est également possible de bloquer les droits d'accès des utilisateurs. Dans les systèmes de traitement automatisé de données, la limitation du traitement devrait être garantie par des mesures techniques, de manière à empêcher tout traitement ultérieur ou modification des données pour des finalités autres que celles découlant de l'al. 3.

Al. 4: mention du caractère litigieux

Cette disposition reprend matériellement le droit en vigueur (art. 25, al. 2, LPD). Elle indique que l'organe fédéral ajoute à la donnée personnelle la mention de son caractère litigieux si l'exactitude ou l'inexactitude de cette donnée ne peut être établie.

Al. 5: procédure selon la loi sur la procédure administrative

L'al. 5 dispose que la procédure par laquelle la personne concernée pourra faire valoir ses prétentions est régie par la loi fédérale du 20 décembre 1968 sur la procédure administrative (PA)[41], tout comme l'indique l'art. 25, al. 4, LPD.

Al. 6: réserve en faveur de dispositions spéciales

L'al. 6 introduit une réserve en faveur des dispositions spéciales d'autres lois fédérales, notamment celles introduites dans le CP, le CPP et le EIMP, sur la base desquelles la personne concernée peut faire valoir des prétentions.

Art. 20 Procédure en cas de communications de documents officiels contenant des données personnelles

L'art. 20 est une norme de coordination entre la LPDS et la loi fédérale du 17 décembre 2014 sur la transparence (LTrans)[42] au niveau de la procédure. Son contenu est identique à celui de l'art. 25bis LPD, sous réserve qu'il renvoie à l'art. 19 LPDS. L'application de cette norme de coordination est toutefois limitée puisque l'art. 3, al. 1, let. a, LTrans prescrit que cette loi ne s'applique pas à l'accès aux documents officiels concernant notamment les procédures pénales (ch. 2), d'entraide judiciaire et administrative internationale et juridictionnelles de droit public, y compris administratives (ch. 5).

2.5 Surveillance

Les art. 21 à 25 transposent les art. 45 à 47 de la directive (UE) 2016/680 et donnent suite aux recommandations adressées par l'Union européenne à la Suisse lors de l'évaluation Schengen de 2014 selon lesquelles des pouvoirs décisionnelles devraient être conférés au préposé.

Art. 21 Préposé fédéral à la protection des données et à la transparence

L'al. 1 prévoit que le préposé est l'autorité compétente pour surveiller l'application des dispositions fédérales de protection des données personnelles. Il peut surveiller les organes fédéraux ainsi que les sous-traitants relevant du champ d'application de la LPDS.

L'al. 2 exclut toutefois certaines autorités du champ de surveillance du préposé, tels que les tribunaux fédéraux (let. a). Ces dérogations se justifient principalement par le fait que la soumission de ces autorités à cette surveillance serait susceptible de nuire à la séparation des pouvoirs et à l'indépendance de la justice. Celles-ci sont compatibles avec les exigences de l'art. 45, par. 2, de la directive (UE) 2016/680.

Selon la let. b, le Ministère public de la Confédération est lui aussi exclu du champ de surveillance du préposé dans la mesure où il traite des données personnelles dans le cadre de procédures pénales[43].

Enfin, selon la let. c, sont exclues du champ de surveillance du préposé les autorités fédérales dans la mesure où elles traitent des données personnelles dans le cadre de procédures d'entraide judiciaire internationale en matière pénale. Cette exception concerne essentiellement le Ministère public de la Confédération et l'Office fédéral de la justice. Selon la déclaration du Conseil fédéral concernant l'art. 1 de la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959[44], l'Office fédéral de la justice doit être considé-

41 RS **172.021**

42 RS **152.3**

43 Voir le considérant 80 de la directive (UE) 2016/680 et l'art. 18 de celle-ci.

44 RS **0.351.1**

ré comme autorité judiciaire suisse aux fins de la convention. La portée de cette exception est toutefois limitée car le préposé peut vérifier la régularité d'un traitement de données lorsqu'une personne concernée fait valoir les droits qui lui sont accordés par l'art. 11*c* EIMP.

Art. 22 Enquête

Cette disposition met en œuvre l'art. 46 par. 1, let. i, de la directive (UE) 2016/680.

Al. 1: ouverture de l'enquête

En vertu de l'al. 1, le préposé est tenu d'ouvrir une enquête d'office ou sur dénonciation dès que des indices font penser que des traitements de données pourraient être contraires à des dispositions légales de protection des données. L'enquête peut être ouverte contre l'organe fédéral responsable ou le sous-traitant comme le prévoit la directive (UE) 2016/680. Le dénonciateur peut être un tiers ou la personne concernée. Il n'a toutefois pas qualité de partie à la procédure, sous réserve de disposition spéciale[45] (voir la réserve formulée à l'art. 25, al. 2, LPDS). Si l'auteur de la dénonciation est la personne concernée, le préposé est tenu de l'informer de la suite donnée à sa dénonciation (al. 4). Pour faire valoir ses droits, la personne concernée doit agir selon les voies de droit applicables, à savoir par voie civile s'il s'agit du sous-traitant ou par voie de recours contre la décision rendue par l'organe fédéral responsable, comme c'est du reste le cas aujourd'hui.

Comme le relève le considérant 82 de la directive (UE) 2016/680, les pouvoirs du préposé ne doivent pas interférer avec les règles spécifiques de procédure, telle la procédure pénale. Dans le cadre de son enquête, celui-ci se limite donc à vérifier la licéité d'un traitement au regard des exigences de protection des données applicables. S'il constate une erreur relative au traitement des données, il peut prendre des mesures administratives à l'encontre de l'organe fédéral concerné ou du sous-traitant (art. 24 LPDS). Tel pourrait être le cas si la sécurité des données n'est pas garantie ou si des tiers non autorisés ont accès aux données.

Al. 2: renonciation à l'ouverture d'une enquête

Le préposé peut renoncer à ouvrir une enquête lorsque la violation des prescriptions de protection des données est de peu d'importance. Cet alinéa peut également s'appliquer si le préposé considère que la fourniture de conseils à l'organe fédéral concerné ou au sous-traitant peut constituer une mesure suffisante pour remédier à une situation en soi peu problématique.

Al. 3: devoirs de collaboration

L'al. 3 règle le devoir de collaboration de l'organe fédéral et du sous-traitant, en reprenant la réglementation prévue aux art. 27, al. 3, et 29, al. 2, LPD. En vertu de cette disposition, la partie à la procédure d'enquête doit fournir au préposé tous les renseignements et documents qui lui sont nécessaires pour son enquête. La seconde phrase de l'al. 3 prescrit que le droit de refuser de fournir des renseignements est régi par les art. 16 et 17 PA. L'art. 16, al. 1, PA renvoie à l'art. 42, al. 1 et 3, de la loi fédérale du 4 décembre 1947 de procédure civile fédérale[46]. Cette disposition prévoit que les personnes interrogées sur des faits dont la révélation les exposerait à des poursuites pénales peuvent refuser de témoigner.

Art. 23 Pouvoirs

Cette disposition correspond aux exigences de l'art. 47, par. 1, de la directive (UE) 2016/680, qui prescrit que les Etats Schengen sont tenus de prévoir que l'autorité de contrôle dispose de pouvoirs d'enquête, notamment celui d'obtenir du responsable du traitement et du sous-

[45] Voir l'art. 349*h*, al. 3 P-CP.

[46] RS **273**

traitant l'accès à toutes les données traitées et à toutes les informations nécessaires pour l'exercice de ses tâches.

Les mesures énumérées à l'al. 1 ne peuvent être ordonnées que si une procédure d'enquête a été ouverte et pour autant que l'organe fédéral ou le sous-traitant ne respecte pas son obligation de collaborer. En d'autres termes, ce n'est que si ses tentatives d'obtenir la collaboration de l'organe fédéral ou du sous-traitant sont restées vaines que le préposé pourra ordonner les mesures prévues aux let. a à d.

La liste des mesures prévues à l'al. 1, non exhaustive, est semblable à celle de l'art. 12 PA. Parmi ses attributions, le préposé peut ordonner l'accès à tous les renseignements, documents, registres d'activités et données personnelles nécessaires pour l'enquête (let. a) ou encore aux locaux et aux installations (let. b). Comme toute autorité fédérale, il doit respecter les dispositions légales applicables, notamment celles sur la protection des données et celles garantissant la confidentialité des secrets d'affaires et de fabrication. Il est également soumis au secret de fonction au sens de l'art. 22 de la loi du 24 mars 2000 sur le personnel de la Confédération (LPers)[47]. La confidentialité des données personnelles auxquelles il a accès dans l'exercice de ses tâches de surveillance est garantie, notamment lorsqu'il informe l'auteur d'une dénonciation de la suite donnée à celle-ci (art. 22, al. 4, LPDS) ou lorsqu'il publie son rapport d'activités en vertu de l'art. 30 LPD.

Al. 2: mesures provisionnelles

L'al. 2 confère au préposé la compétence d'ordonner des mesures provisionnelles pour la durée de l'enquête. Actuellement, l'art. 33, al. 2, LPD autorise le préposé à requérir des mesures provisionnelles du président de la cour du Tribunal administratif fédéral compétente en matière de protection des données s'il constate à l'issue de son enquête que la personne concernée risque de subir un préjudice difficilement réparable. Vu que l'art. 24 LPDS confère des compétences décisionnelles au préposé, l'intervention du Tribunal administratif fédéral pour ordonner des mesures provisionnelles n'est plus nécessaire. La procédure de recours contre les mesures provisionnelles est régie par les art. 44 ss PA. L'art. 55 PA règle l'effet suspensif du recours.

Art. 24 Mesures administratives

L'art. 24 LPDS met en œuvre l'art. 47, par. 2, de la directive (UE) 2016/680.

L'al. 1 laisse une grande marge de manœuvre au préposé puisqu'il ne l'oblige pas à prendre des mesures administratives, mais lui donne la faculté de le faire.

L'art. 24 prévoit une liste de mesures contre des traitements de données contraires à des dispositions de protection des données. Ces mesures vont du simple avertissement (al. 3) jusqu'à l'ordre de détruire des données personnelles (al. 1)

L'al. 2 prescrit en outre que le préposé peut suspendre ou interdire la communication de données personnelles si elle est contraire aux dispositions légales applicables en matière de communications de données personnelles à un Etat tiers ou à un organisme international, soit les art. 349*c* à 349*e* CP. Il est à noter que l'al. 2 ne mentionne pas les communications de données à des Etats Schengen puisque celles-ci sont soumises aux mêmes conditions de protection des données que celles applicables aux communications de données à des autorités pénales suisses (voir l'art. 8, al. 1 LPDS).

Le principe de base de cette réglementation est le respect du principe de proportionnalité. Ainsi, au lieu d'ordonner la cessation du traitement, le préposé peut ordonner sa mise en conformité et limiter la mesure à la partie du traitement problématique.

---

[47] RS **172.220.1**

Le préposé notifie sa décision uniquement à l'organe fédéral ou au sous-traitant partie à la procédure d'enquête sous réserve de l'exception prévue à l'art. 25, al. 2, LPDS. La mesure prononcée doit être motivée de manière précise.

Art. 25 Procédure

Conformément à l'al. 1, la procédure d'enquête et les décisions sur les mesures visées aux art. 23 et 24 sont régies par la PA. L'organe fédéral ou le sous-traitant partie à l'enquête a en particulier le droit d'être entendu (art. 29 ss PA).

L'al. 2 précise que seul l'organe fédéral ou le sous-traitant contre qui une enquête est ouverte a qualité de partie à la procédure. En principe, seuls ceux-ci peuvent recourir contre les mesures prononcées contre eux par le préposé. La personne concernée n'a pas qualité de partie à la procédure, même si le préposé a ouvert l'enquête sur dénonciation de celle-ci. La personne concernée doit donc agir contre l'organe fédéral responsable (art. 19 LPDS), en recourant le cas échéant contre la décision de celui-ci auprès de l'autorité de recours compétente. Cette conséquence est inchangée par rapport au droit en vigueur. L'al. 2 réserve toutefois l'art. 349*h* CP, qui prévoit que la personne concernée peut, à certaines conditions, demander au préposé l'ouverture d'une enquête et recourir, le cas échéant, contre la décision du préposé en qualité de partie.

Quant à l'al. 3, il prescrit que le préposé a qualité pour recourir contre les décisions sur recours du Tribunal administratif fédéral auprès du Tribunal fédéral, comme c'est du reste déjà le cas aujourd'hui en vertu des art. 27, al. 6, et 29, al. 4, LPD.

2.6 Assistance administrative entre le préposé et les autorités étrangères

Art. 26

L'art. 26 LPDS règle l'assistance administrative entre le préposé et les autorités des Etats Schengen chargées de la protection des données. Cette disposition, nouvelle par rapport à la LPD, transpose l'art. 50 de la directive (UE) 2016/680. L'art. 31, al. 1, let. c, LPD se limite à attribuer au préposé la tâche de collaborer avec les autorités étrangères chargées de la protection des données.

Al. 1: conditions

L'al. 1 pose le principe selon lequel le préposé peut échanger des informations ou des données personnelles avec une autorité d'un Etat Schengen chargée de la protection des données pour l'accomplissement de leurs tâches légales respectives, pour autant que certaines conditions, énumérées aux let. a à e, soient remplies.

Selon la première condition (let. a), le principe de réciprocité en matière d'assistance administrative dans le domaine de la protection des données doit être garanti entre la Suisse et l'Etat Schengen. Deuxièmement, conformément au principe de spécialité, les informations et les données personnelles échangées ne doivent être utilisées que dans le cadre de la procédure liée à la protection des données à la base de la demande d'assistance (let. b). Si les données transmises doivent être utilisées ultérieurement dans le cadre d'une procédure pénale, les dispositions sur l'entraide judiciaire internationale en matière pénale s'appliquent. Les troisième et quatrième conditions garantissent le respect des secrets professionnels, d'affaires et de fabrication (let. c) et interdisent que les informations et les données échangées soient communiquées à des tiers sans l'accord préalable de l'autorité qui les a transmises (let. d). Enfin, l'autorité destinataire doit respecter les charges et les restrictions d'utilisation exigées par l'autorité qui lui a transmis les informations (let. e).

Al. 2: communication de données personnelles

L'al. 2 définit aux let. a à g les indications que le préposé peut communiquer à l'autorité de l'Etat Schengen pour motiver sa demande d'assistance administrative ou pour donner suite à une demande d'un Etat Schengen. Le préposé ne peut communiquer l'identité des personnes concernées que si cela est indispensable à l'accomplissement de ses tâches légales ou de celles de l'autorité de l'Etat Schengen (al. 2, let. c).

Al. 3: consultation

Lorsque, dans le cadre d'une procédure d'assistance administrative, le préposé envisage de transmettre à une autorité d'un Etat Schengen chargée de la protection des données des informations susceptibles de contenir des secrets professionnels ou des secrets d'affaires ou de fabrication, il est tenu d'informer les personnes concernées en les invitant à prendre position. Il est néanmoins délié de son obligation si le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés.

2.7 Disposition transitoire concernant les procédures en cours

Art. 27

Pour garantir la sécurité juridique et le respect du principe de la bonne foi, cette disposition prescrit que les enquêtes du préposé pendantes au moment de l'entrée en vigueur de la LPDS, ainsi que les recours contre les décisions de première instance, restent régis par l'ancien droit. Cette notion vise aussi bien les règles matérielles de protection des données que les compétences du préposé, ainsi que les autres normes de procédure applicables.

3 Commentaires des modifications de la LPD

Art. 26, al. 3, 1re phrase

L'al. 3, 1re phrase, concrétise l'indépendance du préposé en précisant qu'il ne doit recevoir ni solliciter d'instructions de la part d'une autorité ou d'un tiers. Cette modification tient compte des exigences de l'art. 42, par. 1 et 2, de la directive (UE) 2016/680.

Art. 26a, al. 1 et 1bis

Actuellement, la période de fonction du préposé peut être reconduite un nombre indéterminé de fois. Ce principe est modifié afin de transposer les exigences de l'art. 44, par. 1, let. e, de la directive (UE) 2016/680, qui prévoit que les Etats Schengen doivent régler le caractère renouvelable ou non renouvelable du mandat du ou des membres de chaque autorité de contrôle et, si c'est le cas, le nombre de mandats. Cette disposition laisse donc le choix aux Etats Schengen de décider si l'autorité de contrôle peut être reconduite ou non dans ses fonctions et, si oui, le nombre de fois.

Conformément à la marge de manœuvre conférée par l'art. 44 de la directive (UE) 2016/680, le préposé peut être reconduit dans ses fonctions deux fois. Ce dernier peut donc rester en fonction pendant douze ans au maximum. Cette mesure permet de renforcer l'indépendance du préposé en tant qu'autorité. La crainte pour le préposé de ne pas être reconduit dans sa fonction ne doit pas constituer un frein à l'accomplissement de ses tâches légales. Si le préposé atteint l'âge de la retraite pendant son mandat, les rapports de travail s'éteignent automatiquement à l'âge fixé à l'art. 21 de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS)[48] (art. 10, al. 1, LPers, par renvoi de l'art. 14, al. 1, LPers).

[48] RS **831.10**

L'al. 1bis correspond à l'al. 1 de l'art. 26*a* LPD, sous réserve de certaines modifications rédactionnelles.

Art. 26b Activité accessoire

L'art. 26*b* renforce les conditions applicables à l'exercice d'une activité accessoire par le préposé. Cette disposition met en œuvre les exigences de l'art. 42, par. 3, de la directive (UE) 2016/680. Elle ne s'applique qu'au préposé. Son suppléant et son secrétariat sont soumis aux dispositions de la LPers.

Alors que l'art. 26*b* LPD se limite à prévoir que le Conseil fédéral peut autoriser le préposé à exercer une autre activité pour autant que son indépendance et sa réputation n'en soient pas affectées, l'al. 1, 1re phrase, pose le principe selon lequel le préposé ne peut exercer aucune autre activité qu'elle soit rémunérée ou non. Cette norme s'écarte de l'art. 41, al. 1, 2ème phrase, P-LPD du Conseil fédéral.

L'al. 2 limite la portée de l'al. 1. Il prévoit que le Conseil fédéral peut autoriser le préposé à exercer une activité accessoire à certaines conditions. La décision du Conseil fédéral est publiée.

Art. 31, al. 1, let. h

Pour tenir compte des exigences de la directive (UE) 2016/680 (art. 46, par. 1, let. b), la liste des attributions du préposé est complétée par une nouvelle tâche. Celui-ci doit ainsi sensibiliser le public à la protection des données.

4 Commentaire relatif à la modification des autres lois fédérales

Les modifications apportées aux autres lois fédérales mettant en œuvre les exigences de la directive (UE) 2016/680 sont commentées dans le message du Conseil fédéral du 15 septembre 2017[49].

[49] FF **2017** 6565, 6766