



31 août 2022

Ordonnance sur la protection des données (OPDo)

Rapport explicatif



Table des matières

1	Contexte	8
1.1	Étapes préalables.....	8
1.2	Présentation de la nLPD.....	8
1.3	Constitutionnalité et compatibilité avec les obligations internationales de la Suisse	10
2	Présentation du projet	11
2.1	Sécurité des données.....	11
2.2	Communication de données personnelles à l'étranger	11
2.3	Droits d'accès.....	12
2.4	Conseiller à la protection des données.....	12
2.5	Exception à l'obligation de tenir un registre des activités de traitement	13
2.6	PF PDT	13
3	Conséquences	13
3.1	Conséquences sur les finances et le personnel de la Confédération et des cantons	13
3.2	Conséquences économiques	14
4	Adaptation du projet soumis à la consultation	15
4.1	Sécurité des données.....	15
4.2	Traitement par le sous-traitant.....	15
4.3	Communication de données personnelles à l'étranger	16
4.4	Obligations du responsable du traitement	16
4.5	Droits de la personne concernée.....	17
4.6	Dispositions particulières pour le traitement de données personnelles par des personnes privées	18
4.7	Dispositions particulières pour le traitement de données personnelles par des organes fédéraux	18
5	Commentaire de l'OPDo	18
5.1	Chapitre 1 : Dispositions générales	18
5.1.1	Section 1 : Sécurité des données	18
5.1.2	Section 2 : Sous-traitance	30
5.1.3	Section 3 : Communication de données personnelles à l'étranger.....	31
5.2	Chapitre 2 : Obligations du responsable du traitement	37
5.3	Chapitre 3 : Droits de la personne concernée.....	39
5.3.1	Section 1 : Droit d'accès.....	40
5.3.2	Section 2 : Droit à la remise et à la transmission des données personnelles	43
5.4	Chapitre 4 : Dispositions particulières pour le traitement de données personnelles par des personnes privées	48
5.5	Chapitre 5 : Dispositions particulières pour le traitement de données personnelles par des organes fédéraux.....	50
5.5.1	Section 1 : Conseiller à la protection des données	50
5.5.2	Section 2 : Devoir d'informer	52
5.5.3	Section 3 : Annonce au PF PDT des projets pour le traitement automatisé des données personnelles	52
5.5.4	Section 4 : Essais pilotes.....	53
5.5.5	Section 5 : Traitements des données à des fins ne se rapportant pas à des personnes	54
5.6	Chapitre 6 : Préposé fédéral à la protection des données et à la transparence	54



5.7	Chapitre 7 : Dispositions finales	59
6	Commentaire relatif à l'annexe 1 (États, territoires, secteurs déterminés dans un État et organismes internationaux dans lesquels un niveau de protection adéquat est garanti).....	60
7	Commentaire relatif à l'annexe 2 (abrogation et modification d'autres actes).....	60
7.1	Abrogation de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données	60
7.2	Aperçu des modifications d'ordonnances sectorielles.....	60
7.3	Ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes	63
7.4	Ordonnance du 4 décembre 2009 sur les mesures de police administrative de l'Office fédéral de la police et sur le système d'information HOOGAN	63
7.5	Ordonnance du 16 août 2017 sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération....	63
7.6	Ordonnance du 24 octobre 2007 relative à l'admission, au séjour et à l'exercice d'une activité lucrative	64
7.7	Ordonnance du 10 novembre 2021 sur le système d'entrée et de sortie	64
7.8	Ordonnance 3 du 11 août 1999 sur l'asile	64
7.9	Ordonnance VIS du 18 décembre 2013	64
7.10	Ordonnance SYMIC du 12 avril 2006	65
7.11	Ordonnance du 20 septembre 2002 sur les documents d'identité	65
7.12	Ordonnance du 14 novembre 2012 sur l'établissement de documents de voyage pour étrangers.....	66
7.13	Ordonnance du 2 novembre 2016 concernant la loi fédérale relative à la convention internationale pour la protection de toutes les personnes contre les disparitions forcées.....	66
7.14	Ordonnance du 8 septembre 1999 sur l'archivage	66
7.15	Ordonnance du 24 mai 2006 sur la transparence.....	66
7.16	Ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration	67
7.17	Ordonnance GEVER du 3 avril 2019.....	67
7.18	Ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération	67
7.19	Ordonnance du 25 novembre 2020 sur la transformation numérique et l'informatique.....	68
7.20	Ordonnance du 19 octobre 2016 sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération	68
7.21	Ordonnance du 20 juin 2018 sur le traitement des données dans le système de gestion des mandats du Service linguistique DFAE.....	68
7.22	Ordonnance du 4 mai 2016 sur les émoluments de fedpol.....	69
7.23	Ordonnance du 12 février 2020 sur les marchés publics	69
7.24	Ordonnance du 29 octobre 2008 sur l'organisation de la Chancellerie fédérale.....	69
7.25	Ordonnance SIVIP du 18 novembre 2015.....	69
7.26	Ordonnance du 25 novembre 1998 concernant l'Etat-major « Prise d'otage et chantage »	69
7.27	Ordonnance du 22 novembre 2017 concernant la protection des données personnelles du personnel de la Confédération.....	69
7.28	Ordonnance Web-DFAE du 5 novembre 2014	70
7.29	Ordonnance du 28 avril 2004 sur l'état civil (OEC).....	70

7.30	Ordonnance du 18 novembre 1992 sur la mensuration officielle	71
7.31	Ordonnance du 17 octobre 2007 sur le registre du commerce	71
7.32	Ordonnance Ordipro du 22 mars 2019	71
7.33	Ordonnance E-VERA du 17 août 2016.....	71
7.34	Ordonnance CV-DFAE du 26 avril 2017.....	72
7.35	Ordonnance « e-vent » du 17 octobre 2018	72
7.36	Ordonnance Plato du 25 septembre 2020	72
7.37	Ordonnance du 26 juin 2013 sur la Commission fédérale chargée de juger les possibilités de traiter les personnes internées à vie.....	72
7.38	Ordonnance du 7 novembre 2012 sur la protection extraprocédurale des témoins	73
7.39	Ordonnance du 20 septembre 2013 relative au système d'information en matière pénale de l'Office fédéral de la douane et de la sécurité des frontières	73
7.40	Ordonnance VOSTRA du 29 septembre 2006.....	73
7.41	Ordonnance GPDA du 23 septembre 2016	74
7.42	Ordonnance du 30 novembre 2001 concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police	74
7.43	Ordonnance JANUS du 15 octobre 2008	74
7.44	Ordonnance RIPOL du 26 octobre 2016	75
7.45	Ordonnance IPAS du 15 octobre 2008	75
7.46	Ordonnance du 6 décembre 2013 sur le traitement des données signalétiques biométriques	76
7.47	Ordonnance du 15 octobre 2008 sur l'index national de police.....	76
7.48	Ordonnance N-SIS du 8 mars 2013.....	77
7.49	Ordonnance du 3 décembre 2004 sur les profils d'ADN	77
7.50	Ordonnance Interpol du 21 juin 2013.....	78
7.51	Ordonnance du 15 septembre 2017 sur les systèmes d'information dans le domaine de la formation professionnelle et des hautes écoles	78
7.52	Ordonnance du 29 novembre 2013 sur l'encouragement de la recherche et de l'innovation	78
7.53	Ordonnance du 30 juin 1993 concernant l'organisation de la statistique fédérale	78
7.54	Ordonnance du 30 juin 1993 sur les relevés statistiques	79
7.55	Ordonnance du 26 janvier 2011 sur le numéro d'identification des entreprises	79
7.56	Ordonnance du 25 juin 2003 sur les émoluments et indemnités perçus pour les prestations de services statistiques des unités administratives de la Confédération.....	79
7.57	Ordonnance du 9 juin 2017 sur le Registre fédéral des bâtiments et des logements.....	80
7.58	Ordonnance du 30 juin 1993 sur le Registre des entreprises et des établissements	80
7.59	Ordonnance du 4 septembre 2013 sur la circulation des espèces de faune et de flore protégées	80
7.60	Ordonnance animex-ch du 1 ^{er} septembre 2010.....	80
7.61	Ordonnance du 4 décembre 2009 concernant le Service de renseignement de l'armée	80
7.62	Ordonnance du 17 octobre 2012 sur la guerre électronique et l'exploration radio	81
7.63	Ordonnance du 4 juillet 2007 concernant la protection des informations	81

7.64	Ordonnance du 21 mai 2008 sur la géoinformation (OGéo)	81
7.65	Ordonnance du 16 décembre 2009 sur les systèmes d'information de l'armée	82
7.66	Ordonnance du 21 novembre 2018 sur la sécurité militaire	82
7.67	Ordonnance du 2 juillet 2008 sur les armes.....	83
7.68	Ordonnance du 11 novembre 2020 sur la protection civile	83
7.69	Ordonnance du 12 août 2015 sur le bureau de notification pour les médicaments vitaux à usage humain.....	83
7.70	Ordonnance du 5 avril 2006 sur les finances de la Confédération	83
7.71	Ordonnance du 1 ^{er} novembre 2006 sur les douanes	84
7.72	Ordonnance du 4 avril 2007 régissant l'utilisation d'appareils de prises de vue, de relevé et d'autres appareils de surveillance par l'Office fédéral de la douane et de la sécurité des frontières.....	84
7.73	Ordonnance du 23 août 2017 sur le traitement des données dans l'OFDF	84
7.74	Ordonnance du 12 octobre 2011 sur la statistique du commerce extérieur.....	84
7.75	Ordonnance du 27 novembre 2009 régissant la taxe sur la valeur ajoutée.....	85
7.76	Ordonnance du 1 ^{er} novembre 2017 sur l'énergie.....	85
7.77	Ordonnance du 9 juin 2006 sur les qualifications du personnel des installations nucléaires	85
7.78	Ordonnance du 9 juin 2006 sur les équipes de surveillance des installations nucléaires.....	85
7.79	Ordonnance du 14 mars 2008 sur l'approvisionnement en électricité	85
7.80	Ordonnance du 30 novembre 2018 sur le système d'information relatif aux accidents de la route	86
7.81	Ordonnance du 30 novembre 2018 sur le système d'information relatif à l'admission à la circulation.....	86
7.82	Ordonnance du 4 novembre 2009 sur la vidéosurveillance dans les transports publics.....	86
7.83	Ordonnance du 17 décembre 2014 sur les enquêtes de sécurité en cas d'incident dans le domaine des transports.....	86
7.84	Ordonnance du 2 septembre 2015 sur la licence d'entreprise de transport de voyageurs et de marchandises par route.....	87
7.85	Ordonnance du 4 novembre 2009 sur le transport de voyageurs	87
7.86	Ordonnance du 18 décembre 1995 sur le service de la navigation aérienne	87
7.87	Ordonnance du 15 novembre 2017 surveillance de la correspondance par poste et télécommunication.....	87
7.88	Ordonnance du 15 novembre 2017 sur le système de traitement pour la surveillance de la correspondance par poste et télécommunication	87
7.89	Ordonnance du 9 mars 2007 sur les services de télécommunication	87
7.90	Ordonnance du 6 octobre 1997 sur les ressources d'adressage dans le domaine des télécommunications	88
7.91	Ordonnance du 5 novembre 2014 sur les domaines Internet	88
7.92	Ordonnance du 4 décembre 2000 sur la procréation médicalement assistée ...	88
7.93	Ordonnance du 14 février 2007 sur l'analyse génétique humaine	88
7.94	Ordonnance du 16 mars 2007 sur la transplantation	88
7.95	Ordonnance du 18 octobre 2017 sur la transplantation croisée	88
7.96	Ordonnance du 16 mars 2007 sur l'attribution d'organes.....	89
7.97	Ordonnance du 20 septembre 2013 relative à la recherche sur l'être humain ..	89
7.98	Ordonnance d'organisation du 20 septembre 2013 concernant la LRH	89
7.99	Ordonnance du 26 novembre 2008 concernant les examens LPMéd.....	90

7.100	Ordonnance du 14 novembre 2018 sur les autorisations dans le domaine des médicaments.....	90
7.101	Ordonnance du 21 septembre 2018 sur les médicaments.....	90
7.102	Ordonnance du 18 août 2004 sur les médicaments vétérinaires	90
7.103	Ordonnance du 1 ^{er} juillet 2020 sur les dispositifs médicaux.....	91
7.104	Ordonnance du 31 octobre 2018 concernant le système d'information sur les antibiotiques en médecine vétérinaire	91
7.105	Ordonnance du 4 mai 2022 sur les dispositifs médicaux de diagnostic in vitro ..	91
7.106	Ordonnance du 27 février 1991 sur les accidents majeurs	91
7.107	Ordonnance du 20 octobre 2021 sur la restitution, la reprise et l'élimination des appareils électriques et électroniques.....	91
7.108	Ordonnance du 22 mars 2017 sur le dossier électronique du patient	91
7.109	Ordonnance du 27 mai 2020 sur l'exécution de la législation sur les denrées alimentaires.....	92
7.110	Ordonnance du 29 avril 2015 sur les épidémies.....	92
7.111	Ordonnance du 29 avril 2015 sur les laboratoires de microbiologie.....	92
7.112	Ordonnance 1 du 10 mai 2000 relative à la loi sur le travail.....	93
7.113	Ordonnance du 19 juin 1995 sur les chauffeurs	93
7.114	Ordonnance du 6 septembre 2006 sur le travail au noir	93
7.115	Ordonnance du 16 janvier 1991 sur le service de l'emploi.....	93
7.116	Ordonnance du 11 septembre 1996 sur le service civil.....	94
7.117	Ordonnance du 20 août 2014 sur le système d'information du service civil	94
7.118	Ordonnance du 11 septembre 2002 sur la partie générale du droit des assurances sociales.....	94
7.119	Règlement du 31 octobre 1947 sur l'assurance-vieillesse et survivants	94
7.120	Règlement du 17 janvier 1961 sur l'assurance-invalidité	94
7.121	Ordonnance du 27 juin 1995 sur l'assurance-maladie	95
7.122	Ordonnance du 20 décembre 1982 sur l'assurance-accidents	95
7.123	Ordonnance du 31 octobre 2007 sur les allocations familiales	95
7.124	Ordonnance du 31 août 1983 sur l'assurance-chômage.....	95
7.125	Ordonnance du 26 mai 2021 sur les systèmes d'information AC.....	96
7.126	Ordonnance du 18 juin 2021 sur les systèmes d'information consulaires du Département fédéral des affaires étrangères.....	96
7.127	Ordonnance du 28 mai 1997 sur les AOP et les IGP	96
7.128	Ordonnance du 22 septembre 1997 sur l'agriculture biologique	96
7.129	Ordonnance du 25 mai 2011 sur les dénominations «montagne» et «alpage» ..	96
7.130	Ordonnance du 3 novembre 2021 relative à Identitas SA et à la banque de données sur le trafic des animaux	97
7.131	Ordonnance du 27 avril 2022 concernant les systèmes d'information de l'OSAV liés à la chaîne agroalimentaire.....	97
7.132	Ordonnance du 18 novembre 2015 réglant les échanges d'importation, de transit et d'exportation d'animaux et de produits animaux avec les pays tiers ..	97
7.133	Ordonnance du 26 juin 2013 sur l'obligation des prestataires de services de déclarer leurs qualifications professionnelles dans le cadre des professions réglementées et sur la vérification de ces qualifications	97
7.134	Ordonnance du 24 juin 2015 sur les prestations de sécurité privées fournies à l'étranger	97
7.135	Ordonnance du 12 août 2015 sur le système de traitement des données relatives aux prestations de sécurité privées	98

7.136	Ordonnance du 7 novembre 2018 sur les jeux d'argent.....	98
7.137	Ordonnance du 27 novembre 2000 sur les explosifs	98
7.138	Ordonnance du 25 août 2004 sur le Bureau de communication en matière de blanchiment d'argent	99

1 Contexte

1.1 Étapes préalables

À la suite d'une évaluation de la loi fédérale du 19 juin 1992 sur la protection des données¹ (LPD), et compte tenu des évolutions technologiques et des développements du droit européen, le Conseil fédéral a décidé de réviser la loi. Le 15 septembre 2017, il a ainsi adopté le message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales². Le projet de loi comprend d'une part une révision totale de la LPD (nLPD) et d'autre part une révision partielle d'autres lois fédérales, afin de mettre en œuvre la directive (UE) 2016/680³ notamment. Le Parlement a décidé que la mise en œuvre du projet du Conseil fédéral se ferait en deux étapes. Dans la première étape, seule la directive Schengen (UE) 2016/680 sur la protection des données dans le droit pénal a été mise en œuvre : la loi fédérale du 28 septembre 2018 sur la protection des données Schengen (LPDS)⁴ est entrée en vigueur le 1^{er} mars 2019. Lors de la deuxième étape, le Parlement a délibéré sur la nouvelle loi sur la protection des données (nLPD)⁵ et l'a adoptée le 25 septembre 2020.

En raison de la révision totale de la LPD, les ordonnances qui lui sont associées, à savoir l'ordonnance relative à la loi fédérale sur la protection des données (OLPD)⁶ et l'ordonnance sur les certifications en matière de protection des données (OCPD)⁷ doivent également être adaptées.

1.2 Présentation de la nLPD

La nLPD règle le traitement de données personnelles concernant des personnes physiques effectué par des personnes privées ou des organes fédéraux (art. 2, al. 1). Elle ne s'applique toutefois pas aux données qu'une personne physique traite pour son usage exclusivement personnel (art. 2, al. 2, let. a). La nLPD prévoit en outre une exception pour les traitements de données effectués par les Chambres fédérales et les commissions parlementaires dans le cadre de leurs délibérations (art. 2, al. 2, let. b), ainsi que par les bénéficiaires institutionnels qui jouissent en Suisse de l'immunité de juridiction (art. 2, al. 2, let. c). Les traitements de données personnelles effectués dans le cadre de procédures devant des tribunaux ou dans le cadre de procédures régies par les dispositions de la procédure fédérale, ainsi que les droits des personnes concernées, obéissent au droit de procédure applicable. La nLPD s'applique par contre aux procédures administratives de première instance (art. 2, al. 3). Les registres publics relatifs aux rapports de droit privé sont régis principalement par les dispositions spéciales des lois fédérales applicables (art. 2, al. 4). Un article relatif au champ d'application territorial de la nLPD a été ajouté par le Parlement. Cette disposition (art. 3) précise que la loi s'applique aussi aux états de fait qui se sont produits à l'étranger lorsqu'ils déploient des effets en Suisse. Elle renvoie en outre à la loi fédérale du 18 décembre 1987 sur

¹ RS 235.1

² FF 2017 6565

³ 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.

⁴ RS 235.3

⁵ FF 2020 7397

⁶ RS 235.11

⁷ RS 235.13

le droit international privé (LDIP)⁸. Enfin, l'art. 4 rappelle le rôle du Préposé fédéral à la protection des données et à la transparence (PFPDT).

Le deuxième chapitre contient des dispositions générales sur le traitement de données personnelles.

L'art. 5 dresse un catalogue de définitions. Notons notamment que la nouvelle loi remplace la notion de maître du fichier par celle de responsable du traitement (art. 5, let. j, nLPD). Le concept du profilage à risque élevé (art. 5, let. g) a été introduit ultérieurement, par les Chambres fédérales.

L'art. 6 fixe certains principes généraux à respecter. Tout traitement de données personnelles doit être licite (art. 6, al. 1) et respecter les principes de la bonne foi et de la proportionnalité (art. 6, al. 2). La collecte de données personnelles doit poursuivre des finalités déterminées et reconnaissables pour la personne concernée (art. 6, al. 3). Les données doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement (art. 6, al. 4). Celui qui traite des données personnelles doit également s'assurer de l'exactitude des données (art. 6, al. 5). Le responsable du traitement et le sous-traitant sont tenus de protéger les données dès la conception et par défaut (*privacy by design and by default* ; art. 7), et d'assurer la sécurité des données personnelles (art. 8). En vertu de l'art. 10, les responsables du traitement peuvent nommer un conseiller à la protection des données. Ils doivent également établir un registre des activités de traitement (art. 12).

L'art. 9 règle la sous-traitance de données personnelles. La nLPD codifie l'instrument des codes de conduite (art. 11).

Une section a été introduite au chapitre 2 par le Parlement. Elle est consacrée aux traitements de données personnelles par des responsables du traitement privés qui ont leur siège ou leur domicile à l'étranger. L'art. 14 instaure la notion du représentant et l'art. 15 définit ses obligations.

La section 3 du chapitre 2 porte sur la communication des données à l'étranger. Des données personnelles ne peuvent être communiquées à l'étranger que si le Conseil fédéral a constaté que l'État concerné ou l'organisme international concerné offre un niveau de protection adéquat (art. 16). L'art. 17 prévoit néanmoins différentes exceptions.

Le chapitre 3 règle les obligations du responsable du traitement. Il précise le devoir d'informer les personnes concernées lors de la collecte de données personnelles (art. 19 à 20). L'art. 21 introduit une nouvelle obligation d'information pour les décisions individuelles automatisées. L'art. 22 introduit l'obligation d'effectuer une analyse d'impact relative à la protection des données personnelles. Le responsable du traitement a en outre l'obligation de consulter préalablement le PFPDT lorsque l'analyse d'impact relative à la protection des données révèle que, malgré les mesures prévues par le responsable du traitement, le traitement présente encore un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 23). Enfin, le responsable du traitement doit annoncer au PFPDT les violations de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 24).

⁸ RS 291

Les droits de la personne concernée sont inscrits au chapitre 4. Le droit d'accès et ses restrictions sont réglés aux art. 25 à 27. Quant au droit à la portabilité et ses restrictions, consacrés aux art. 28 et 29, ils ont été introduits par le Parlement.

Le chapitre 5 contient un certain nombre de dispositions applicables au traitement de données personnelles par des personnes privées. La nLPD interdit ainsi aux personnes privées qui traitent des données personnelles de porter une atteinte illicite à la personnalité des personnes concernées (art. 30, al. 1) et en particulier de traiter des données personnelles en violation des principes définis aux art. 6 et 8 nLPD ou contre la volonté expresse de la personne concernée en l'absence de motif justificatif (art. 30, al. 2, let. a et b et art. 31). Ce chapitre règle en outre les prétentions de droit civil que les personnes lésées peuvent faire valoir (art. 32).

Un sixième chapitre (art. 33 à 42) régit le traitement de données personnelles par des organes fédéraux. Ceux-ci ne sont en principe en droit de traiter des données personnelles que s'il existe une base légale (art. 34, al. 1). L'art. 41 règle les prétentions que les personnes concernées peuvent faire valoir à l'encontre d'un organe fédéral responsable d'un traitement les concernant.

L'organisation et les compétences du PFPDT sont définies au chapitre 7. L'élection du chef du PFPDT (le préposé) est le fait de l'Assemblée fédérale (art. 43, al. 1). Cette nouvelle procédure a été introduite par les Chambres fédérales. La durée, le renouvellement du mandat, ainsi que la fin des rapports de fonction sont réglés à l'art. 44 tandis que l'art. 47 régit les activités accessoires. La question du budget du PFPDT (art. 45) et des incompatibilités en lien avec la fonction de préposé (art. 46) a été ajoutée par le Parlement. Un dernier article vient clore cette première section relative à l'organisation du PFPDT : il s'agit de l'art. 48 portant sur l'autocontrôle du PFPDT. Une deuxième section porte sur les enquêtes que peut mener le PFPDT. Il est ainsi prévu qu'il ouvre d'office ou sur dénonciation une enquête contre un organe fédéral ou une personne privée si des indices suffisants font penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données (art. 49, al. 1). Le PFPDT a certains pouvoirs (art. 50) et peut prendre des mesures administratives (art. 51). La section 3 contient les dispositions sur l'assistance administrative entre le PFPDT et d'autres autorités en Suisse (art. 54), ou des autorités étrangères (art. 55). La nLPD confère également d'autres tâches au PFPDT (art. 56 à 58), en particulier la tenue d'un registre des activités de traitement des organes fédéraux (art. 56). Pour certaines prestations fournies à des personnes privées, le PFPDT perçoit des émoluments (art. 59).

Enfin, la nLPD contient un catalogue de dispositions pénales relatives à la violation de différentes obligations légales (chap. 8, art. 60 à 66), ainsi qu'un catalogue de dispositions finales (chap. 10, art. 68 à 74) dont on peut, en particulier, mentionner la disposition transitoire relative aux données concernant des personnes morales (art. 71) qui est d'importance pour l'adaptation des ordonnances sectorielles (cf. annexe 2 de la présente ordonnance).

La révision totale de la LPD conduit à la modification de nombreuses lois sectorielles. Plusieurs ordonnances doivent également être modifiées sur la base de la révision de l'OLPD.

1.3 Constitutionnalité et compatibilité avec les obligations internationales de la Suisse

L'ordonnance relative à la loi fédérale sur la protection des données est une ordonnance d'exécution de la loi fédérale sur la protection des données telle qu'elle a été révisée par le Parlement le 25 septembre 2020. En ce sens, l'ordonnance respecte la loi et il peut être

renvoyé aux explications contenues dans le message pour ce qui concerne les aspects juridiques (cf. FF 2017 6565, spécialement 6796 ss).

2 Présentation du projet

Les principales nouveautés liées à la modification de l'OLPD sont brièvement décrites ci-dessous. L'ordonnance relative à la loi fédérale sur la protection des données (OLPD) s'appellera désormais ordonnance sur la protection des données (OPDo)

2.1 Sécurité des données

L'art. 8, al. 3, nLPD oblige le Conseil fédéral à définir des exigences minimales en matière de sécurité des données personnelles. La nouvelle réglementation se fonde sur les standards en matière de sécurité des données actuellement fixés aux art. 8 ss. de l'OLPD. Les dispositions sont toutefois retravaillées et complétées pour correspondre à l'état actuel des technologies et répondre aux exigences de la directive (UE) 2016/680 qui relève de l'acquis Schengen. La compatibilité avec le règlement européen sur la protection des données (RGPD) revêt également une importance centrale, afin que les entreprises suisses actives dans l'Union européenne qui garantissent une sécurité des données conforme au RGPD puissent partir du principe qu'elles remplissent aussi les exigences minimales en Suisse.

L'ordonnance ne pose pas d'exigences minimales strictes en matière de sécurité des données qui s'appliqueraient uniformément à tous : une réglementation de cette sorte ne serait pas praticable. Tout comme l'art. 8, al. 1, nLPD, qui évoque une sécurité adéquate des données personnelles par rapport au risque encouru, l'ordonnance suit, elle aussi, une approche fondée sur le risque : le responsable doit établir le besoin de protection et déterminer les mesures à prendre en fonction du risque. L'ordonnance précise les critères à prendre en compte et fournit une ligne directrice quant à la façon de concevoir les mesures (art. 1, 2 et 3 OPDo).

Le responsable du traitement privé et son sous-traitant privé devront au moins journaliser l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction lors de traitements automatisés de données sensibles à grande échelle ou de profilage à risque élevé, lorsque les mesures préventives ne suffisent pas à garantir la protection des données et lorsque, sans cette mesure, il ne serait pas possible de vérifier a posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées. L'organe fédéral responsable et son sous-traitant devront quant à eux journaliser l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des traitements automatisés de données personnelles. Pour les traitements de données qui n'entrent pas dans le champ d'application de la directive (UE) 2016/680, il a été prévu un délai transitoire de trois ans ou au plus tard jusqu'à la fin du cycle de vie du système. Enfin, la durée de conservation des procès-verbaux de journalisation est d'au moins une année (art. 4 OPDo).

Les responsables du traitement devront continuer d'établir un règlement de traitement (art. 5 s. OPDo).

2.2 Communication de données personnelles à l'étranger

La section portant sur les communications de données personnelles à l'étranger a été entièrement revue. En effet, selon la nLPD, le Conseil fédéral déterminera quels États ou organismes internationaux garantissent un niveau de protection adéquat. Pour cette raison, l'ordonnance fixe désormais les critères dont le Conseil fédéral devra tenir compte dans son évaluation (art. 8 OPDo). Un tableau énumérant les États et organismes internationaux

qui garantissent un niveau de protection adéquat figure à l'annexe 1. Le niveau de protection sera réévalué périodiquement après l'entrée en vigueur de l'ordonnance (art. 8, al. 4, OPDo).

Par ailleurs, l'ordonnance concrétise les autres possibilités de garantir un niveau de protection approprié citées à l'art. 16, al. 2, nLPD (p. ex. les clauses type de protection des données) (art 9 ss. OPDo).

Enfin, le Conseil fédéral fait usage de la norme de délégation prévue à l'art. 16, al. 3, nLPD, au sens de laquelle il peut prévoir d'autres garanties appropriées. Ainsi, les données personnelles pourront être communiquées si un niveau de protection approprié est garanti par un code de conduite ou une certification (art. 12 OPDo).

2.3 Droits d'accès

Comme dans le droit en vigueur, les demandes d'accès devront en principe se faire par écrit ou par voie électronique. En revanche, les requérants pourront faire valoir leurs droits d'accès un peu plus facilement dans la mesure où ils auront la possibilité de faire leur demande par oral, moyennant l'accord du responsable du traitement.

D'autres dispositions d'exécution concernant les droits d'accès sont en partie reprises du droit actuel. Ainsi, la disposition portant sur le délai est uniquement modifiée du point de vue terminologique et systématique (art. 18 OPDo). Les exceptions à la gratuité du droit d'accès (art. 19 OPDo) sont restées dans l'ensemble les mêmes, si ce n'est que l'absence d'un intérêt légitime a été biffée, parce qu'elle constitue, selon l'art. 26, al. 1, let. c, nLPD, un motif de refus de communiquer des renseignements.

En revanche, la consultation de données d'une personne décédée n'est pas reprise dans l'OPDo. Régler cette question au niveau d'une ordonnance n'était en effet pas adéquat et le Parlement a refusé d'introduire un projet d'article à ce sujet dans la nLPD.

Un droit à la remise ou à la transmission des données personnelles a été instauré dans le cadre de la révision de la loi. À cet effet, de nouvelles dispositions ont été établies (art. 20 s. OPDo). Toutefois, la plupart des dispositions d'exécution du droit d'accès s'appliquent par analogie (art. 22 OPDo).

2.4 Conseiller à la protection des données

Bien qu'en français le terme de « conseiller à la protection des données » soit resté le même, en allemand, il est adapté pour passer de « Datenschutzverantwortlicher » (art. 12a et 12b OLPD) et « Berater für den Datenschutz in den Departementen und der Bundeskanzlei » (art. 23 OLPD) à « Datenschutzberaterin bzw. Datenschutzberater ». Il y a des normes distinctes, l'une portant sur le conseiller à la protection des données d'un responsable du traitement privé (art. 23 OPDo) et les autres concernant le conseiller à la protection des données des organes fédéraux (art. 25 ss OPDo).

Puisque les exigences auxquelles est soumis le conseiller à la protection des données d'un responsable du traitement privé, ainsi que ses tâches principales, sont déjà réglées à l'art. 10 nLPD, la disposition de l'ordonnance qui s'y rapporte (art. 23 OPDo) se limite à décrire les exigences que doit remplir un responsable du traitement s'il fait appel un conseiller à la protection des données.

En revanche, la réglementation relative au conseiller à la protection des données des organes fédéraux est conservée. À la différence de l'ancien droit, il est prévu que chaque organe fédéral désigne un conseiller, et non plus uniquement les départements et la Chancellerie fédérale. Plusieurs organes fédéraux pourront désigner un conseiller commun : cela permettra en particulier aux plus petits organes et à ceux avec une structure organisationnelle particulière de ne pas perdre des synergies et d'économiser des ressources. Les

exigences que le conseiller à la protection des données des organes fédéraux doit remplir sont réglées de la même manière que celles relatives aux conseillers privés, dans la mesure où elles peuvent raisonnablement s'appliquer aux organes fédéraux, et leurs tâches sont pour l'essentiel identiques.

2.5 Exception à l'obligation de tenir un registre des activités de traitement

Afin de décharger sur le plan administratif les PME qui n'effectuent pas de traitements présentant certains risques, l'art. 12, al. 5, nLPD délègue au Conseil fédéral la compétence de prévoir des exceptions à l'obligation de tenir un registre des activités pour les entreprises comptant moins de 250 employés. L'ordonnance prévoit une telle exception à moins que le traitement présente certains risques (p. ex. le traitement de données sensibles à grande échelle) (art. 24 OPDo). Le catalogue y figurant est fondé sur la définition de la notion de « risque élevé » au sens de l'analyse d'impact sur la protection des données de l'art. 22, al. 2, nLPD.

2.6 PFPDT

Même si la réglementation relative au PFPDT a subi d'importants changements dans la nLPD, les dispositions relatives à son siège ainsi qu'aux relations et à la communication avec les autres autorités ont pu être reprises moyennant de légères modifications (voir art. 36 à 38 OPDo). Selon la nouvelle procédure d'élection, le chef du PFPDT (le préposé) sera élu par l'Assemblée fédérale (art. 43, al. 1, nLPD) ; le 27 janvier 2022, dans le cadre de l'initiative parlementaire 21.443, la CIP-N a adopté un projet d'ordonnance de l'Assemblée fédérale contenant les dispositions d'exécution relatives aux rapports de travail du préposé. Des modifications ponctuelles sont en outre prévues dans la nLPD. Le Parlement a accepté le projet en votation finale le 17 juin 2022. Les rapports de travail du secrétariat permanent du PFPDT resteront quant à eux inscrits dans l'OPDo et continueront d'être régis par la loi du 24 mars 2000 sur le personnel de la Confédération (LPers)⁹ et ses dispositions d'exécution (art. 36, al. 2, OPDo).

La base légale permettant le traitement des données par le PFPDT est désormais réglementée de manière plus détaillée (art. 39 OPDo). Dans le droit en vigueur, elle n'est décrite que de façon générale, dans le contexte du système de gestion des affaires. En outre, l'art. 48 nLPD prescrit que le PFPDT doit effectuer un autocontrôle afin de garantir le respect des dispositions fédérales de protection des données en son sein. Les mesures d'autocontrôle sont décrites dans l'ordonnance (art. 40 OPDo) : il doit établir un règlement pour tous les traitements automatisés.

3 Conséquences

3.1 Conséquences sur les finances et le personnel de la Confédération et des cantons

Ce n'est que dans le cadre des normes de délégation de la nLPD et de la compétence d'exécution du Conseil fédéral que l'OPDo entraîne des conséquences pour la Confédération :

- L'adaptation des exigences minimales en matière de sécurité des données induira un certain coût de mise en œuvre pour les responsables du traitement. Il devrait toutefois rester limité pour les responsables privés, car l'essentiel de la réglementation est une reprise du droit en vigueur, à l'exception d'adaptations ponctuelles. Pour les organes fédéraux,

⁹ RS 172.220.1

c'est en particulier l'extension de l'obligation de journalisation qui engendrera des coûts supplémentaires : en effet, il faudra procéder à des adaptations ponctuelles des systèmes et davantage de capacités de stockage seront nécessaires. L'extension de l'obligation de journaliser doit être vue comme un développement des mesures fixées par le Conseil fédéral en 2009 (voir l'arrêté du Conseil fédéral du 16 décembre 2009 concernant les mesures visant à renforcer la sécurité de l'information au sein de l'administration fédérale) Les coûts ne peuvent pas encore être déterminés avec certitude et ils devront être intégrés au budget des unités administratives concernées. Afin de tenir compte de ces dépenses supplémentaires, un délai transitoire de 3 ans est prévu pour la mise en application de la journalisation des traitements de données qui ne tombent pas dans le champ d'application de la directive (UE) 2016/680. Par ailleurs, les procès-verbaux de journalisation devront être conservés au moins 1 an et non pas 2 ans, délai initialement proposé dans l'avant-projet.

- Le fait que chaque organe fédéral doive nommer un conseiller à la protection des données peut aussi entraîner des coûts supplémentaires. Toutefois, cette augmentation devrait être limitée par le fait qu'un grand nombre d'offices fédéraux disposent déjà d'un conseiller à la protection des données. Dans certaines circonstances, des organes fédéraux devront toutefois allouer davantage de ressources à leurs conseillers, car leur cahier des charges et les exigences auxquelles ils seront soumis seront plus vastes que dans le droit actuel. Le montant des ressources nécessaires pourrait varier en fonction de la taille des organes fédéraux et de leurs missions. En revanche, le renforcement du rôle du conseiller à la protection des données pourrait contribuer à décharger le PFPDT.

Au sein de la Confédération, les conséquences en termes de finances et de personnel se ressentiront principalement au niveau du PFPDT car celui-ci devra remplir de nouvelles fonctions en application de la nLPD. L'Office fédéral de la justice (OFJ) sera aussi concerné dans une moindre mesure car de nouvelles tâches lui incomberont, notamment l'évaluation du niveau de protection des données d'autres États et organes internationaux. Le message du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales (FF 2017 6565, 6784 ss.) prévoyait également une augmentation des ressources nécessaires pour le PFPDT et l'OFJ.

Le projet ne concerne pas les cantons et les communes. Seules les personnes privées et les organes fédéraux entrent dans le champ d'application de la nLPD (art. 2, al. 1, nLPD), et donc de l'OPDo.

3.2 Conséquences économiques

Les entreprises sont principalement concernées par les conséquences de la révision totale de la LPD. Ces conséquences ont été prises en compte et décrites dans l'analyse d'impact de la réglementation sur la LPD¹⁰. Les conséquences de l'OPDo, qui sont indépendantes de la révision de la LPD et n'ont pas été étudiées dans le cadre de cette analyse d'impact, devraient surtout concerner la sécurité des données. Ces conséquences devraient être d'une importance limitée, car les obligations concrètes des entreprises n'ont été que légèrement modifiées. Les mesures prévues contribuent par ailleurs à renforcer la cybersécurité, ce qui profitera aux entreprises. Un certain effort de mise en œuvre reste à prévoir. Les changements requis dépendront du risque que comportent les traitements de données effectués par une entreprise. Les entreprises moins concernées par la réglementation sur la protection des

¹⁰ Analyse d'impact de la réglementation (AIR) du 11 juin 2016 concernant la révision de la loi fédérale sur la protection des données (LPD) (disponible en allemand sur : <http://www.seco.admin.ch> > Secrétariat d'État à l'économie SECO > Services et publications > Publications > Réglementation > Analyse d'impact de la réglementation > AIR approfondies > Loi sur la protection des données (LPD) (2016)).

données devront prendre moins de mesures que les autres. Cette approche offre une certaine marge de manœuvre aux entreprises.

De plus, la révision totale de la législation sur la protection des données est aussi significative pour l'économie car son entrée en vigueur est d'une grande importance dans le cadre de l'évaluation en cours de la Suisse par la Commission européenne. Le maintien de la décision d'adéquation de l'UE est crucial pour la place économique suisse et sa compétitivité. Les États membres de l'UE ne pourront continuer de communiquer des données personnelles à la Suisse sans entrave supplémentaire que si elle reste reconnue par l'UE comme un État tiers avec un niveau de protection des données adéquat. Sans décision d'adéquation de l'UE (et sans libre circulation des données), la Suisse subirait une importante perte de compétitivité. L'adaptation du droit suisse de la protection des données à la Convention 108 du Conseil de l'Europe, qui a été modernisée, est aussi importante en matière d'accès aux marchés internationaux. En outre, au niveau international, l'intérêt des États non-européens à adhérer à la version modernisée de la Convention 108 sur la protection des données augmente : l'échange de données entre la Suisse et ces États sera potentiellement facilité.

Enfin, un traitement sûr des données personnelles renforce la confiance du public envers les technologies numériques et leurs fournisseurs. Une meilleure protection des données permet donc de promouvoir la numérisation.

4 Adaptation du projet soumis à la consultation

Le projet d'ordonnance soumis à la consultation a été retravaillé tant au niveau du contenu que de la systématique. Les prochains chapitres détaillent les principales adaptations effectuées.

4.1 Sécurité des données

La section relative à la sécurité des données a été retravaillée pour tenir compte des critiques exprimées lors de la consultation.

Les notions sujettes à interprétations ont été supprimées (par exemple « intervalles appropriés »). En outre, les objectifs font désormais l'objet d'un article distinct (art. 2 OPDo), qui s'inspire de la loi fédérale sur la sécurité de l'information au sein de la Confédération¹¹. L'art. 3 règle les mesures techniques et organisationnelles.

Les articles relatifs à la journalisation et au règlement de traitement (art. 4 à 6 OPDo) conservent, dans la mesure du possible, la formulation de l'OLPD en vigueur. Ainsi le renvoi à l'analyse d'impact sur la protection des données est supprimé des conditions d'assujettissement à l'obligation de journaliser. La proposition d'augmenter la durée de conservation des procès-verbaux de journalisation à deux ans n'est pas retenue. Cependant, comme la durée d'un an, prévue dans l'OLPD en vigueur, constitue à la fois un minimum et un maximum, le terme "au moins" a été ajouté pour permettre aux personnes privées de conserver les procès-verbaux de journalisation durant plus qu'un an. Pour les organes fédéraux, le droit spécial est réservé.

4.2 Traitement par le sous-traitant

La teneur de l'art. 6 P-OLPD a été supprimée. À la place de cet article, l'art. 7 OPDo règle seulement le type d'autorisation préalable grâce à laquelle le responsable du traitement

¹¹ LSI, FF 2017 2907

peut habiliter un sous-traitant à confier le traitement des données à un tiers. Cette disposition s'appuie sur l'art. 22, al. 2 de la directive (UE) 2016/680 et l'art. 28, al. 2, RGPD. Pour des motifs de sécurité du droit, elle reprend ce que le Conseil fédéral avait expliqué au sujet de l'autorisation de la sous-traitance dans le message relatif à la loi sur la protection des données (voir FF 2017 6565, 6651).

Les al. 1 et 2 de l'art. 6 P-OLPD ont été biffés parce que ces normes sont déjà couvertes par l'art. 9, al. 1, let. a, nLPD ainsi que par les dispositions relatives à la communication de données personnelles à l'étranger (art. 16 s. nLPD ; art. 8 ss OPDo). Même en confiant le traitement des données personnelles à un sous-traitant, c'est au responsable qu'incombe la protection des données.

Par ailleurs, il ne semblait pas nécessaire de régler expressément le fait que l'autorisation préalable de sous-traitement par un organe fédéral doit être approuvée par écrit, comme cela était prévu à l'art. 6, al. 3, P-OLPD. Il faut toutefois partir du principe que cette forme est à privilégier dans l'optique de la sécurité juridique. En outre, il convient de respecter, le cas échéant, les exigences formelles applicables en droit des marchés publics.

L'art. 7 P-OLPD a été entièrement supprimé. Cette suppression est motivée par le fait que l'art. 26, al. 2, let. a, OPDo (ancien art. 28, al. 2, let. a et b, P-OLPD) règle déjà la question de la participation du conseiller à la protection des données.

4.3 Communication de données personnelles à l'étranger

Les résultats de la consultation externe ont montré un besoin de transparence et de clarté.

Désormais, les évaluations du Conseil fédéral doivent être publiées conformément à l'art. 8, al. 5, OPDo. Une disposition transitoire règle les modalités (art. 46, al. 2 OPDo). En outre, le principe de transparence a été expressément ajouté à l'art. 9, al. 1, let. a, OPDo.

Finalement, un délai de 90 jours est précisé concernant la prise de position du PFPDT au sujet des clauses types de protection des données et des règles d'entreprise contraignantes qui lui sont annoncées (art. 10, al. 2, et art. 11, al. 3, OPDo).

4.4 Obligations du responsable du traitement

Le sous-traitant a été supprimé dans le nouvel art. 13, al. 1, OPDo (ancien art. 13, al. 1, P-OLPD), parce que la base légale de l'art. 19 nLPD s'applique uniquement au responsable du traitement, auquel revient le devoir d'informer. L'al. 1 est par ailleurs modifié dans le sens du RGPD. L'al. 2 de l'ancien art. 13 P-OLPD a été supprimé. Il ressort de la consultation que l'utilisation de pictogrammes dans la forme qui était exigée était impossible à appliquer pour les milieux économiques. L'exigence de la lisibilité par une machine en particulier a été véhémentement critiquée.

L'art. 15 P-OLPD ne s'appliquera plus qu'aux organes fédéraux, raison pour laquelle il est déplacé dans le chapitre relatif au traitement de données personnelles par des organes fédéraux (nouvel art. 30 OPDo). Cette disposition reste valable pour les organes fédéraux conformément aux exigences posées à l'art. 7, al. 2 de la directive (UE) 2016/680.

L'art. 16 P-OLPD est supprimé parce que l'article correspondant dans la loi a été supprimé suite à la consultation et qu'il ne figurait plus dans la version soumise au Parlement. Le conserver dans le projet d'ordonnance aurait été incohérent.

L'art. 17 P-OLPD a aussi été supprimé : l'art. 21, al. 2, nLPD en particulier couvre déjà le but et le sens de cette disposition.

L'art. 14 OPDo (ancien art. 18 P-OLPD) se contente de régler la conservation de l'analyse d'impact relative à la protection des données personnelles et ne mentionne plus sa forme. La forme sous laquelle les responsables souhaitent la conserver est laissée à leur appréciation, comme il en va pour d'autres instruments réglementés dans la nLPD ou l'OPDo. Il faudra sans nul doute qu'elle puisse être lue, et donc qu'elle soit enregistrée dans un format couramment utilisé, en vue de sa vérification par le PFPDT ou en cas de violation de la sécurité des données.

L'al. 2 de l'art. 15 P-OLPD est complété en fonction des prescriptions de l'art. 24, al. 1 nLPD, afin que les informations manquantes soient communiquées « dans les meilleurs délais ». L'al. 4 est supprimé en raison de la modification aux art. 26 et 27 OPDo selon l'organe fédéral devra informer conseiller à la protection des données en cas de violation de la sécurité des données.

4.5 Droits de la personne concernée

Dans la section 1 portant sur le droit d'accès, l'art. 20, al. 4, P-OLPD (nouvel art. 16 al. 5, OPDo) a été modifié de telle façon que les exigences prévues à l'art. 1, al. 2, let. a et b OLPD en vue de garantir la sécurité des informations transmises ne sont reprises que partiellement. L'obligation du responsable du traitement de garantir que les données de la personne soient protégées de l'accès de tiers non autorisé lors de la communication des renseignements qui était fixée à la let. b de l'art. 20 P-OLPD est supprimée, car elle ressort déjà suffisamment clairement de l'art. 8 nLPD. On conserve dans l'OPDo le devoir du responsable de prendre des mesures adéquates pour assurer l'identification de la personne concernée, celle-ci étant tenue de collaborer.

L'art. 20, al. 5, P-OLPD est biffé car l'art. 26, al. 4, nLPD suffit à traiter la problématique. Cet article de la nLPD prévoit que le responsable du traitement doit indiquer le motif pour lequel il refuse, restreint ou diffère la communication des informations. Cette disposition est suffisante pour que la personne concernée puisse faire valoir son droit à l'information en justice si nécessaire. Les responsables n'ont donc plus d'obligation de conserver la documentation, mais la conservation pourrait leur servir à titre de preuve.

Une modification a été apportée à l'art. 21 P-OLPD (nouvel art. 17 OPDo) afin qu'il soit clair qu'il s'agit d'une norme de coordination. L'al. 2 est modifié : le sous-traitant devra aider le responsable du traitement à fournir les renseignements.

L'art. 23 P-OLPD (nouvel art. 19 OPDo) portant sur les exceptions à la gratuité est également modifié. L'al. 3 prévoit que la demande est considérée comme retirée lorsque la personne ne la confirme pas dans les 10 jours après qu'elle ait été informée de la participation aux coûts. Le délai de réponse prévu à l'art. 18 OPDo (ancien art. 22 P-OLPD) commence par conséquent à courir après ce délai de réflexion.

La section 2 relative au droit à la remise ou à la transmission des données personnelles a une nouvelle fois été remaniée en profondeur. De nouveaux articles ont été ajoutés : l'art. 20 OPDo concerne l'étendue du droit et l'art. 21, les exigences techniques de mise en œuvre. Sous le titre de délais, modalités et responsabilité, l'art. 22 OPDo (ancien art. 24 P-OLPD) fixe dans quelle mesure les dispositions relatives au droit d'accès peuvent s'appliquer au droit à la remise ou à la transmission des données personnelles.

4.6 Dispositions particulières pour le traitement de données personnelles par des personnes privées

L'al. 1 de l'art. 25 P-OLPD (nouvel art. 23 OPDo) « Conseiller à la protection des données » est supprimé parce que les responsables du traitement privés ne sont pas obligés de nommer un conseiller. Une lettre c a été ajoutée à la partie de l'article qui est conservée : elle introduit le droit du conseiller à la protection des données d'informer l'organe supérieur de direction ou d'administration dans les cas importants.

4.7 Dispositions particulières pour le traitement de données personnelles par des organes fédéraux

Il est précisé à l'al. 2 de l'art. 26 OPDo (ancien art. 28 P-OLPD) que le conseiller à la protection des données participe à l'application des règles de protection des données. Les ch. 1 et 2 servent uniquement à titre d'illustration.

La tâche du conseiller à la protection des données d'annoncer au PFPDT les violations de la sécurité des données (art. 28, al. 2, let. c, P-OLPD) est désormais considérée comme étant un devoir de l'organe fédéral. Elle figure de ce fait à l'art. 27 OPDo.

L'art. 31 P-OLPD relatif à l'information du conseiller à la protection des données est supprimé. La disposition reprenait en partie l'art. 20, al. 2, OLPD. Toutefois, cette information au conseiller à la protection des données découle de ses tâches générales de conseil, de soutien et de contrôle.

5 Commentaire de l'OPDo

5.1 Chapitre 1 : Dispositions générales

5.1.1 Section 1 : Sécurité des données

La loi pose les garde-fous permettant de garantir la sécurité des données. D'après l'art. 8, al. 1, nLPD, les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru. Selon l'al. 2, ces mesures doivent permettre d'éviter toute violation de la sécurité des données. Enfin, l'al. 3 charge le Conseil fédéral de préciser les exigences minimales en matière de sécurité des données au niveau de l'ordonnance.

Le Conseil fédéral remplit le mandat légal prévu à l'art. 8, al. 3, nLPD via les dispositions sur la sécurité des données de l'OPDo. La disposition pénale de l'art. 61, let. c, nLPD renvoie également à ces exigences minimales. Le degré de sécurité à respecter pour ne pas violer la disposition pénale dépend des principes et des critères définis dans la section 1 de l'ordonnance. Seule une infraction commise intentionnellement est punissable au sens de l'art. 61, let. c, nLPD. Cela présuppose donc que le responsable ne respecte pas, en connaissance de cause et de manière délibérée, les exigences minimales en matière de sécurité des données. Par exemple, une personne serait punissable si elle n'installait pas de logiciel antivirus, alors qu'elle sait (ou du moins accepte) qu'elle prend des mesures insuffisantes pour se conformer aux exigences minimales de sécurité des données.

Il a été renoncé à inscrire des exigences minimales strictes dans l'OPDo car la loi suit une approche fondée sur le risque et qu'il est impossible de fixer des exigences minimales générales applicables à chaque branche. L'approche suivie dans l'OPDo repose plutôt sur le fait qu'il incombe en premier lieu au responsable du traitement de déterminer quelles sont les

mesures nécessaires dans un cas précis, et de les prendre. Ces mesures ne peuvent être prises qu'au cas par cas, et leur portée dépend du risque encouru. En toute logique, les exigences sont plus élevées pour un hôpital qui traite régulièrement des données sensibles que pour une boulangerie ou une boucherie qui traite les données de ses clients ou de ses fournisseurs. L'OPDo contient surtout des lignes directrices permettant de déterminer les mesures à prendre (art. 1, 2 et 3 OPDo). Cela permet de garantir la flexibilité nécessaire pour couvrir le large éventail de cas et éviter un excès de réglementation, en particulier pour les entreprises pour lesquelles les traitements de données sont rares et présentent peu de risques.

Contrairement au RGPD, le droit suisse n'a pas prévu de devoir général de responsabilité (« accountability »). Toutefois le droit suisse connaît déjà en droit actuel des mesures qui permettent de remplir les exigences de responsabilité ou d'« accountability ». Il s'agit d'une part de la journalisation (art. 4) et d'autre part du règlement de traitement (art. 5 et 6). Ces deux mesures sont reprises dans l'OPDo. Elles sont déterminantes pour que le droit suisse puisse garantir un niveau de protection adéquat par rapport à celui de l'UE. En outre, la journalisation est exigée par la directive (UE) 2016/680. Ces deux mesures constituent des exigences minimales de sécurité au sens de l'art. 8, al. 3, nLPD. Le Conseil fédéral continue de suivre une approche fondée sur le risque : plus les droits de la personnalité et les droits fondamentaux de l'individu sont menacés, plus les exigences sont élevées.

Dans le droit en vigueur, les exigences minimales en matière de sécurité des données sont réglées aux art. 8 à 12 et 20 à 21 OLPD. Le Conseil fédéral a décidé de se fonder sur les dispositions actuelles dans le projet de révision : les dispositions de droit matériel sont en principe reprises telles quelles. Des adaptations ont uniquement été effectuées lorsqu'elles semblaient nécessaires en raison de la numérisation ou des progrès techniques, des dispositions de la loi révisée, ou de la directive (UE) 2016/680, plus précisément ses art. 25 et 29. En outre, le Conseil fédéral s'est appuyé sur le règlement (UE) 2016/679 afin que les entreprises suisses actives dans l'Union européenne qui garantissent une sécurité des données conforme au RGPD puissent aussi partir du principe qu'elles remplissent les exigences minimales en Suisse.

Du point de vue systématique, la sécurité des données est réglée dans une section qui lui est dédiée. Dans l'OLPD actuelle, la sécurité des données est traitée séparément pour les personnes privées et les organes fédéraux : par souci de clarté et pour une meilleure lisibilité, ces dispositions ont été rassemblées. Lorsqu'elles sont différentes pour les personnes privées et les organes fédéraux, elles sont réglées dans des articles ou des alinéas distincts.

Art. 1 Principes

L'art. 1 OPDo règle les principes à respecter lorsqu'il s'agit de déterminer les mesures visant à garantir la sécurité des données. Il reprend globalement les concepts de l'art. 8, al. 2 et 3, en détaillant certains aspects. L'al. 1 de l'art. 8 OLPD a en revanche été supprimé car les objectifs visant à garantir la sécurité des données sont désormais fixés au niveau de la loi : l'art. 8, al. 2, nLPD dispose que les mesures doivent permettre d'éviter toute violation de la sécurité des données. D'après l'art. 5, let. h, nLPD, il y a violation dès lors qu'il y a une perte, une modification, un effacement, une destruction, une divulgation ou un accès non autorisé aux données, de manière accidentelle ou illicite, conformément aux objectifs de protection du domaine informatique que sont la confidentialité, l'intégrité, la disponibilité et la traçabilité.

D'après l'art. 8, al. 1, nLPD, les responsables du traitement et les sous-traitants doivent assurer une sécurité adéquate des données par rapport au risque encouru. L'art. 1 OPDo reprend cet objectif de protection dans un nouvel al. 1. La disposition fixe, en outre, différents critères permettant, d'une part, d'évaluer le besoin de protection (al. 2) et, d'autre part, d'évaluer les risques pour la personne concernée ou ses droits fondamentaux (al. 3). Un quatrième alinéa précise encore que des critères supplémentaires peuvent être pris en compte au moment de déterminer quelles sont les mesures techniques et organisationnelles nécessaires pour garantir la sécurité adéquate des données (al. 4). La liste des critères s'inspire du droit en vigueur.

L'art. 1, al. 2, OPDo reprend sur le fond l'art. 8, al. 2, let. a et b, OLPD et le complète afin de régler l'analyse du besoin de protection. Celui-ci se définit sur la base du type de données traitées et de la finalité, de la nature, de l'étendue et des circonstances du traitement des données. Il s'agit en particulier du niveau de protection qui doit être garanti au vu de la mise en danger des droits de la personnalité et des droits fondamentaux des personnes concernées. Plus le besoin de protection est élevé, plus les exigences relatives aux mesures sont strictes. Pour évaluer le besoin de protection, il convient de tenir compte des critères suivants :

- Le type de données traitées (let. a) : il est par exemple déterminant de savoir si des données personnelles sensibles (art. 5, let. c, nLPD) sont traitées.
- La finalité, la nature, l'étendue et les circonstances du traitement des données (let. b) : la finalité s'attache au but du traitement et, plus particulièrement, à examiner si le but du traitement entraîne un risque accru pour les droits de la personnalité et les droits fondamentaux ; la nature du traitement s'intéresse à examiner comment sont traitées les données. Le besoin de protection peut par exemple être plus élevé dans le cas d'une prise de décision entièrement automatisée (utilisation de l'intelligence artificielle) ; l'étendue du traitement est notamment en lien avec le nombre de personnes concernées par le traitement (par exemple données traitées à grande échelle ou surveillance systématique de grandes parties du domaine public). L'utilisation d'un Cloud favorise un besoin de protection plus important que des données stockées sur un serveur interne sans accès externe possible. Le terme de « circonstances » a été ajouté à la let. b, pour qu'elle corresponde à l'art. 22, al. 2, nLPD. Il s'agit d'aspects propres au cas d'espèce qui méritent un regard particulier notamment en raison des effets sur les autres critères. Il permet d'intégrer des critères qui n'entreraient pas dans la définition de ceux déjà mentionnés.

L'art. 1, al. 3, OPDo reprend plus en détail l'art. 8, al. 2, let. c, OLPD. Il introduit l'examen du risque d'atteinte à la personnalité ou aux droits fondamentaux de la personne concernée. Il fixe, comme à l'alinéa précédent, un certain nombre de critères. Cet alinéa est reformulé afin qu'il soit clair que les causes du risque (let. a), les principales menaces (let. b), les mesures prises ou prévues pour réduire les risques (let. c) et la gravité et la probabilité d'une violation de la sécurité des données (let. d) sont décisives. Il s'agit d'un examen en « cascade ». Le résultat de l'évaluation d'un critère est déterminant pour avancer dans l'examen du risque. Ces différents points sont détaillés ici.

- Les causes du risque (let. a). Il s'agit de pouvoir identifier qui sont les personnes (par exemple un responsable informatique, un utilisateur, un concurrent) ou quels sont les événements (par exemple un incendie, un virus informatique) qui pourraient être à la base du risque.
- Les principales menaces (let. b). Ce critère permet de s'interroger quant aux menaces qui pourraient conduire à des violations de la sécurité des données (données perdues, abîmées, modifiées, utilisées de manière inadéquate ou frauduleuse, etc.).

- Les mesures prises ou prévues pour réduire le risque (let. c). Les différentes mesures techniques et organisationnelles qui peuvent être prévues ou prises pour réduire le risque sont précisées à l'art. 3 OPDo.

La gravité et la probabilité d'une violation de la sécurité des données, malgré les mesures prises ou prévues (let. d). Il convient d'identifier quels seraient les impacts possibles sur les personnes concernées lorsque, par exemple, des personnes accèdent de manière illégitime à des données (et les divulguent), les modifient (conduisant à de fausses informations relatives à la personne concernée) ou les suppriment (risquant ainsi de perdre des données nécessaires ; on pense ici par exemple à un dossier médical dont certaines données auraient été détruites, empêchant ainsi un traitement médical adéquat). Plus la probabilité d'une violation de la sécurité des données est élevée et plus les conséquences sur la personne concernée sont importantes, plus les exigences relatives aux mesures sont élevées. Il convient toutefois de relever que toute violation de la sécurité des données au sens de l'art. 5, let. h, nLPD ne constitue pas une violation des exigences minimales au sens de l'art. 8, al. 3, nLPD et donc une violation des devoirs de diligence au sens de l'art. 61, let. c, nLPD. On ne peut ni ne doit exiger une sécurité absolue. Il est en effet concevable que le responsable du traitement ait pris toutes les mesures adéquates, mais que la sécurité des données soit malgré tout violée en raison du risque résiduel ; cela ne saurait être imputé au responsable. Dans le cadre des exigences minimales, il importe surtout de vérifier si le responsable du traitement et le sous-traitant ont pris des mesures adéquates dans le cas concret, qu'il y ait eu une violation de la sécurité des données ou non.

Inspiré de l'art. 8, al. 2, let. d, OLPD, l'art. 1, al. 4, OPDo introduit encore d'autres critères dont il peut être tenu compte lors de la détermination des mesures techniques et organisationnelles visant à garantir une sécurité adéquate des données. Le terme « détermination » comprend un aspect « évaluation » et un aspect « décision » (la terminologie française ne connaît pas d'équivalent exact en allemand). Les critères sont les suivants: l'état des connaissances (let. a) et les coûts de mise en œuvre (let. b). Ces éléments ne renseignent qu'indirectement sur l'opportunité et l'adéquation des mesures à prendre :

- L'état des connaissances (let. a). Les mesures doivent être fixées, ou adaptées, en fonction de l'état actuel des connaissances techniques et scientifiques. Il suffit d'utiliser des mesures déjà disponibles et qui ont prouvé leur efficacité. On ne saurait exiger le recours à des techniques ultramodernes, pas encore testées, ou qui sont encore en cours de développement.
- Les coûts de mise en œuvre (let. b). La notion de « coûts » se comprend au sens large. Elle ne se limite pas aux coûts financiers, mais comprend également les ressources en personnel et en temps nécessaires. Cette terminologie reprend celle du droit européen (directive (UE) 2016/680 et RGPD). Ces coûts sont un critère d'évaluation de l'adéquation des mesures, dans le droit en vigueur aussi – comme il ressort du « Commentaire de l'Office fédéral de la justice à l'appui de l'ordonnance du 14 juin 1993 (état au 1^{er} janvier 2008) relative à la loi fédérale sur la protection des données (OLPD, RS 235.11) », ch. 6.1.1¹². Il faut toutefois commencer par déterminer quelles sont les mesures techniques et organisationnelles nécessaires compte tenu des critères des let. a à c. Les responsables du traitement et les sous-traitants ne peuvent pas se soustraire à l'obligation d'assurer une sécurité des données adéquate au motif que cela occasionne des coûts excessifs ; au contraire, ils doivent toujours être en mesure de garantir une sécurité adéquate. L'absence d'un concept au moment du développement n'est pas non plus un argument pouvant justifier que les coûts

¹² Disponible sur : <https://www.edoeb.admin.ch/edoeb/fr/home/le-pfpdt/bases-legales.html>.

d'implémentation du moyen de mise en œuvre de la sécurité des données sont trop élevés une fois que le système est mis en service. Si l'on est en présence d'un système hérité, il faut tenir compte du temps nécessaire jusqu'à son remplacement (cycle de vie). Le critère des coûts signifie en revanche que lorsqu'il existe plusieurs mesures permettant de garantir un niveau de protection des données adéquat en toutes circonstances, on puisse privilégier la variante la plus économique¹³.

Diverses mesures peuvent être prises pour assurer la sécurité des données. En voici trois exemples :

- Anonymisation, pseudonymisation et chiffrement des données personnelles : l'anonymisation sert surtout à diminuer les éventuelles conséquences négatives qui pourraient affecter une personne dont les données personnelles auraient été divulguées sans son autorisation. Si les données sont anonymisées, la LPD ne s'applique pas.
- Procédure d'identification, d'analyse et d'évaluation des risques et évaluation de l'adéquation des mesures : au-delà d'un certain degré de risque, il peut être judicieux ou parfois même nécessaire d'implémenter une procédure et des processus standardisés qui permettent non seulement de réexaminer régulièrement les risques et l'adéquation des mesures, mais aussi de les évaluer. Toutes ces mesures sont particulièrement importantes en présence de systèmes automatisés : elles contribuent à garantir la sécurité des données sur le long terme et elles permettent de fournir plus facilement une preuve de cette sécurité.
- Formation et conseils aux personnes chargées de la mise en œuvre des mesures : le Conseil fédéral considère que cette mesure est importante car la mise en œuvre et l'efficacité de la sécurité des données dépendent des personnes qui appliquent les mesures définies. Un manque de formation et une absence d'informations pourraient entraîner une violation de la sécurité des données. Par exemple, les collaborateurs devraient recevoir des instructions concernant le risque d'ouvrir un malware.

En fin de compte, ce sont les circonstances du cas individuel qui déterminent le choix des mesures.

Selon l'art. 1, al. 5, et comme dans le droit en vigueur, les mesures doivent être régulièrement réexaminées et, le cas échéant, adaptées. Il faudra en particulier vérifier si les mesures sont toujours appropriées au vu du risque, et si elles sont efficaces. Plutôt que d'avoir lieu de façon « périodique », cet examen devra se faire « pendant toute la durée du traitement ». La fréquence de cet examen dépend du risque pour les droits de la personnalité et les droits fondamentaux des personnes concernées : plus il est élevé, plus il faudra réexaminer les mesures de manière continue. La nouvelle formulation va dans le sens d'un réexamen constant. Elle laisse, toutefois, une grande marge d'appréciation au responsable du traitement et au sous-traitant. Un réexamen peut en outre s'imposer lorsqu'une violation de la sécurité des données s'est produite ou que les modalités du traitement des données ont changé. L'art. 1, al. 5, précise en outre que ce ne sont pas seulement les mesures techniques et organisationnelles qui doivent être réévaluées pendant toute la durée du traitement, soit pendant tout le cycle de vie des données personnelles, mais également le besoin de protection et les risques encourus. L'examen du besoin de protection et des risques encourus permet de vérifier (indirectement) que les mesures techniques et organisationnelles sont appropriées.

¹³ Voir aussi BRUNO BAERISWYL, in: Stämpfli Handkommentar, Datenschutzgesetz, 1^{ère} édition 2015, n° 26 ad art. 7.

Art. 2 Objectifs

L'art. 2 OPDo complète l'art. 1 nLPD, relatif au but de la loi, et concrétise les objectifs visant à garantir la sécurité adéquate des données, désormais fixés à l'art. 8, al. 2, nLPD, qui dispose que les mesures doivent permettre d'éviter toute violation de la sécurité des données. La sécurité absolue est un idéal inatteignable. L'approche fondée sur les risques tend à identifier les risques (art. 1 OPDo) pour adapter et sélectionner les mesures selon les objectifs. Le responsable du traitement et le sous-traitant doivent déterminer les objectifs et l'ampleur de la protection.

La doctrine et la pratique retiennent généralement quatre objectifs de protection connus sous l'acronyme (C.A.I.D.) : la confidentialité, l'authentification, l'intégrité et la disponibilité des données. S'inspirant de l'art. 32 RGPD et dans un souci d'harmonisation avec la loi fédérale sur la sécurité de l'information au sein de la Confédération¹⁴ qui devrait prochainement entrer en vigueur, l'art. 2 a pour objectif la réglementation de la confidentialité (let. a), de la disponibilité (let. b), de l'intégrité (let. c) et de la traçabilité (let. d).

- La confidentialité (let. a) : seules les personnes autorisées peuvent avoir accès aux données personnelles. Le cercle des personnes autorisées est défini par le contexte dans lequel les tâches sont exécutées, de même que par le contenu et l'importance des données. Le cercle de ces personnes peut être très étendu ou extrêmement restreint. Par confidentialité, il convient également de comprendre l'authentification, les méthodes y relatives ainsi que les systèmes de gestion et de limitation des accès pour assurer la sécurité des données. Enfin, il sied d'assurer la confidentialité du système et des données.
- La disponibilité (let. b) : par cet objectif, le responsable du traitement veille à ce que les données puissent être consultées en tout temps. Cette exigence est d'autant plus élevée lorsque les informations doivent être disponibles en permanence pour l'accomplissement de tâches essentielles, voire des tâches légales.
- L'intégrité (let. c) : cet objectif assure l'exactitude des données. Il a son importance, notamment lorsque les données sont destinées au public ou destinées à être réutilisées. Par intégrité, il sied de comprendre l'authenticité, l'imputabilité et l'incontestabilité des données. Ces termes sont parfois utilisés dans la pratique ou la doctrine en lieu et place de l'intégrité.
- La traçabilité (let. d) : cet objectif permet d'identifier tout accès non autorisé, voire toute éventuelle utilisation abusive. Il permet, en outre, de déterminer l'origine d'un incident. Le responsable du traitement assure l'enregistrement des événements et des traces qui ont lieu et veille à ce que ceux-ci ne puissent être altérés. La traçabilité du traitement a son importance en matière de procédure (preuve) et permet également de favoriser les contrôles et la surveillance. L'imputabilité et l'incontestabilité des données sont également utilisées en pratique pour parler des mécanismes de traçabilité.

Ces objectifs tendent à l'élaboration de procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures prises (art. 1, al. 5, et art. 3 OPDo).

Art. 3 Mesures techniques et organisationnelles

L'art. 8, al. 1, nLPD exige qu'une sécurité adéquate des données personnelles soit assurée. Pour tenir compte des résultats de la consultation externe, l'art. 3 prévoit que des mesures organisationnelles et techniques doivent être prises afin d'atteindre les objectifs de l'art. 2. Dans le respect du principe de la proportionnalité, les mesures seront déterminées sur cette

¹⁴ Message du Conseil fédéral du 22 février 2017 concernant la loi sur la sécurité de l'information (LSI), FF 2017 2765. Pour le texte soumis au vote final du Parlement fédéral, cf. FF 2020 9665.

base, en fonction de chaque cas. Les responsables du traitement et les sous-traitants doivent déterminer quelles mesures seront appropriées pour respecter les objectifs de protection. Il est tout à fait concevable que tous les objectifs de protection ne soient pas pertinents dans tous les cas. Si un objectif n'est pas pertinent, les responsables du traitement et les sous-traitants doivent être en mesure de le justifier. Le caractère « approprié » de la mesure dépend des circonstances. De manière didactique, cet article offre un panel de mesures au responsable du traitement et au sous-traitant pour atteindre les objectifs de l'article 2. Une mesure peut, par ailleurs, servir différents objectifs.

Cet article reprend en grande partie l'art. 9 OLPD à quelques modifications près. Les dispositions figurent désormais sous le titre « Mesures techniques et organisationnelles ». L'art. 3 OPDo permet à la Suisse de répondre aux exigences de l'art. 29 de la directive (UE) 2016/680.

En vertu de l'art. 1, al. 3, let. c, OPDo, le responsable du traitement est tenu de prendre des mesures techniques et organisationnelles pour réduire le risque. L'ordonnance fait plusieurs fois référence aux personnes « autorisées » dans le contexte des mesures techniques et organisationnelles. Cela ne présuppose toutefois pas nécessairement l'implication directe d'une personne. On peut aussi inclure les cas dans lesquels des données personnelles sont traitées automatiquement par une application ou dans un système d'information.

L'art. 3, al. 1, OPDo concrétise l'art. 2, al. 1, let. a, OPDo et présente des mesures relatives à la confidentialité ; c'est-à-dire des mesures visant à garantir le contrôle de l'accès aux données (let. a), de l'accès aux locaux et aux installations (let. b) ainsi que le contrôle de l'utilisation (let. c).

- La lettre a règle la question du contrôle de l'accès aux données. Cet objectif de protection reprend celui de l'art. 9, al. 1, let. g, OLPD. Il s'agit principalement de définir les droits d'accès réglant le type et l'étendue des accès en veillant à ce que les personnes autorisées n'aient accès qu'aux données à caractère personnel sur lesquelles porte leur autorisation. Les mesures à mettre en place sont autant d'ordre organisationnel que d'ordre technique.
- La lettre b règle le contrôle de l'accès aux locaux et aux installations, qui figurait auparavant à l'art. 9, al. 1, let. a, OLPD. Les personnes non autorisées n'auront pas accès aux locaux et aux installations utilisées pour le traitement de données personnelles. Le terme « Anlagen » est une nouveauté dans la version allemande, qui n'utilisait auparavant que celui d'« Einrichtungen ». Le français mentionnait déjà quant à lui les « locaux et [...] installations ». Avec le terme « locaux », il convient de comprendre que l'accès aux installations de traitement mobiles doit également être empêché. Cela couvre une large variété d'appareils : des serveurs physiques, installés dans un endroit fixe, en passant par les ordinateurs, les téléphones portables, et les tablettes, à tous les appareils pouvant servir au traitement de données personnelles. Avec les avancées techniques, l'« installation » peut autant concerner l'installation physique que l'installation virtuelle. Il sera par exemple possible d'utiliser des alarmes ou des racks de serveurs (armoires) verrouillables.
- La lettre c reprend le contrôle d'utilisation qui figurait à l'art. 9, al. 1, let. f, OLPD. Le but est d'éviter l'utilisation par des personnes non autorisées des systèmes de traitement automatisés de données personnelles au moyen d'installations de transmission. Les mesures veillent à ce que les données ne puissent être subtilisées ou transférées sans droit. Les mesures possibles sont par exemple les contrôles réguliers des autorisations (p. ex. en bloquant certaines autorisations suite à un changement de personnel ou à la modification des tâches d'une personne), l'installation de programmes contre les virus et les logiciels espions ou encore la sensibilisation du personnel par exemple contre les méthodes d'hameçonnage (phishing).

En matière de disponibilité et d'intégrité, l'art. 3, al. 2, OPDo reprend et se fonde sur les objectifs de l'art. 2, al. 1, let. b et c, OPDo. Les mesures y relatives visent à garantir le contrôle des supports de données (let. a), de la mémoire (let. b), du transport (let. c) ainsi que la restauration (let. d). Les mesures doivent être propres à assurer la disponibilité, la fiabilité et l'intégrité (let. e). Enfin, la sécurité du système doit être maintenue à jour (let. f).

- La lettre a de l'al. 2 traite du contrôle des supports de données qui est actuellement défini à l'art. 9, al. 1, let. b, OLPD. Elle dispose que les personnes non autorisées ne pourront pas lire, copier, modifier, déplacer, effacer ou détruire des supports de données. Il faut surtout éviter que des données personnelles soient transférées sur des supports de données (p. ex. disques durs, clés USB) sans que cela ne soit contrôlé. Les services en ligne, de type cloud, sont aussi considérés comme des supports de données. On pourra par exemple crypter ces supports ou les détruire de façon appropriée. Cette lettre correspond à l'exigence de l'art. 29, par. 2, let. b de la directive (UE) 2016/680.
- La lettre b correspond à l'actuel art. 9, al. 1, let. e, OLPD et concerne le contrôle de la mémoire. La mesure exige que les personnes non autorisées ne puissent pas enregistrer, lire, modifier, effacer ou détruire des données personnelles dans la mémoire (contrôle de la mémoire). Pour faire respecter cet objectif, on pourra établir différents niveaux de droits d'accès aux données, aux applications et aux systèmes d'exploitation, et journaliser les accès aux applications. Cette lettre correspond à l'exigence de l'art. 29, par. 2, let. c, de la directive (UE) 2016/680.
- La lettre c aborde le contrôle du transport (actuellement art. 9, al. 1, let. c, OLPD). En ce sens, il faut empêcher les personnes non autorisées de lire, copier, modifier, effacer ou détruire des données personnelles lors de leur communication ou lors du transport de supports de données. Le responsable du traitement et les sous-traitants doivent faire en sorte que le destinataire des données les reçoive sous leur forme originale, et qu'aucun tiers ne puisse les intercepter. Les exigences concernant les mesures à prendre sont particulièrement élevées dans le cadre du traitement de données sensibles. Le chiffrement des données ou de supports est notamment une mesure efficace.
- La lettre d concerne la possibilité de restaurer la disponibilité des données personnelles et l'accès à ces données en cas d'incident physique ou technique. Elle a été ajoutée à la liste sur la base de l'art. 32, par. 1, let. c du règlement (UE) 2016/679 et correspond aux exigences de l'art. 29, par. 2, let. i de la directive (UE) 2016/680. L'une des mesures possibles consiste en l'élaboration et l'application d'un concept de sauvegarde.
- La lettre e dispose que toutes les fonctions du système de traitement automatisé des données doivent être disponibles (disponibilité), que les dysfonctionnements éventuels doivent être signalés (fiabilité) et que les données personnelles stockées ne doivent pas pouvoir être endommagées par des dysfonctionnements du système (intégrité des données). Elle a été ajoutée à la liste sur la base de l'art. 32, par. 1, let. b du règlement (UE) 2016/679 et correspond aux exigences de l'art. 29, par. 2, let. j de la directive (UE) 2016/680. Il faut garantir la stabilité et la résilience des systèmes utilisés dans la durée. Le système doit signaler les dysfonctionnements lui-même afin que les responsables du traitement et les sous-traitants en soient automatiquement informés. Signaler un dysfonctionnement ne signifie pas automatiquement que les fonctionnalités sont fiables, encore faut-il que le dysfonctionnement soit corrigé.
- La lettre f porte sur la garantie de la sécurité des systèmes d'exploitation et des logiciels d'application utilisés pour le traitement des données personnelles. Comme le traitement est basé sur des systèmes et diverses applications qui en dépendent, il est nécessaire que leur niveau de sécurité soit maintenu à jour et de remédier rapidement aux lacunes critiques. La lettre f complète les dispositions des lettres d et e dans l'objectif de garantir une sécurité globale. Il n'est pas obligatoire d'installer immédiatement chaque mise à jour des systèmes ou des applications, mais il faut qu'un processus soit mis en place (*vulnerability and*

patch management). Les mises à jour de sécurité peuvent être mises en œuvre de manière échelonnée, en fonction des niveaux de risques critiques ou non (élevé, moyen, faible). Des mesures devront être prises pour s'assurer du maintien de la sécurité des données jusqu'à ce que les vulnérabilités soient corrigées. Contrairement à l'art. 3, al. 3, let. c, la lettre f ne porte pas sur des mesures devant être prises en réaction à un problème, mais sur des mesures proactives visant à remédier aux vulnérabilités avant qu'une violation de la sécurité des données n'ait été constatée.

L'al. 3 énonce les mesures de traçabilité (art. 2, al. 1, let. d, OPDo), c'est-à-dire des mesures visant à garantir le contrôle de la saisie (let. a), de la communication (let. b) ainsi que des mesures de détection et réparation (let. c).

- La lettre a règle désormais le contrôle de la saisie. Conformément à ce qui figurait à l'art. 9, al. 1, let. h, OLPD, elle dispose qu'il doit être possible de vérifier a posteriori l'identité des personnes saisissant des données personnelles dans le système de traitement automatisé des données, ainsi que les données saisies ou modifiées et le moment de leur saisie ou modification. L'objectif de protection a été complété pour couvrir les modifications : il est explicitement écrit que la modification de données personnelles doit pouvoir être vérifiée a posteriori. Un des moyens d'assurer cette vérification est la journalisation.
- La lettre b porte sur le contrôle de la communication. Elle reprend l'art. 9, al. 1, let. d, OLPD, avec une formulation légèrement différente. D'après la nouvelle let. b, il doit être possible de vérifier à qui des données personnelles sont communiquées à l'aide d'installations de transmission. Les mesures prises à cet effet doivent permettre d'identifier les destinataires des données. Dans certaines circonstances, connaître l'organe en tant que tel peut être suffisant, sans que la personne physique ne doive forcément être identifiable. Au besoin, il faudra pouvoir justifier à l'aide des procès-verbaux quelles données personnelles ont été communiquées, à qui et par quel moyen.
- La lettre c exige que les responsables du traitement et les sous-traitants puissent rapidement détecter les violations de la sécurité des données au sens de l'art. 5, let. h, nLPD et qu'ils puissent prendre des mesures pour en réduire ou éliminer les conséquences. Contrairement à la let. e de l'al. 2, la let. c concerne principalement les mesures prises en réaction à un problème par les responsables du traitement et les sous-traitants.

L'art. 9, al. 2, OLPD est supprimé car le Conseil fédéral ne l'estime plus nécessaire. Les motifs justifiant de refuser, restreindre ou différer une demande d'accès sont définis dans la loi (voir art. 26 nLPD). Ainsi, selon la nLPD, les responsables et les sous-traitants devront veiller à ce que les personnes concernées puissent effectivement exercer leurs droits et ce, indépendamment des technologies utilisées pour traiter leurs données personnelles.

Art. 4 Journalisation

La journalisation est régie à l'art. 10 OLPD, qui s'applique aussi aux organes fédéraux en raison de la première phrase de l'art. 20, al. 1, OLPD. L'art. 4 OPDo reprend cette réglementation sous une nouvelle forme. La journalisation constitue une mesure au sens de l'art. 3 OPDo. Elle compense le fait que le droit suisse ne prévoit pas, comme le RGPD, un devoir général d'« accountability ». Certaines autorités de protection des données européennes recommandent d'ailleurs cette mesure¹⁵. En outre, la journalisation constitue une mesure classique de prévention en matière de cybersécurité.

¹⁵ Voir, par exemple, CNIL, Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation.

L'objectif de la journalisation est de pouvoir vérifier le traitement des données personnelles a posteriori, afin de déterminer si des données ont été perdues, effacées, détruites, modifiées ou divulguées. La journalisation peut aussi fournir des renseignements permettant de savoir si les données personnelles ont été traitées conformément aux finalités et permettre de veiller à une sécurité adéquate des données. Elle sert en outre à déceler et à faire la lumière sur les violations de la sécurité des données. Elle n'est en revanche pas destinée à surveiller la façon dont les utilisateurs traitent les données personnelles. La journalisation est un processus automatisé. De nos jours, rares sont les systèmes d'information ou de traitements automatisés ne bénéficiant pas d'une journalisation des données traitées.

Selon l'art. 4, al. 1, OPDo, la journalisation s'impose au responsable du traitement privé et à son sous-traitant privé en cas de traitements automatisés de données sensibles à grande échelle ou de profilage à risque élevé, lorsque les mesures préventives ne suffisent pas à garantir la protection des données et lorsque, sans cette mesure, il ne serait pas possible de vérifier a posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées. Ce sont au moins les opérations d'enregistrement, de modification, de lecture, de communication, d'effacement et de destruction des données qui doivent être journalisées. La « lecture » doit être comprise comme un accès sans « modification », il suffit donc de consigner les accès aux données personnelles et les modifications de ces données. Cela suffit à la journalisation de la « lecture ». La phrase « Lorsque les mesures préventives ne suffisent pas à garantir la protection des données » est reprise du droit actuel. Elle a une faible portée en pratique, dès lors qu'il est peu fréquent que les mesures préventives suffisent.

Selon l'al. 2, l'organe fédéral responsable et son sous-traitant journalisent, lors du traitement automatisé de données personnelles, au moins l'enregistrement, la modification, la lecture, la communication, l'effacement ou et la destruction des données. Ce sont les mêmes opérations que celles imposées aux responsables du traitement privés, mais dans des circonstances plus nombreuses (lors de tout traitement automatisé). Cela permet de respecter les exigences de l'art. 25 de la directive (UE) 2016/680 dans le cadre de la coopération instaurée par Schengen dans le domaine pénal. Comme expliqué précédemment, il suffit de journaliser les accès aux données personnelles et les modifications de ces données en ce qui concerne la « lecture ». Pour mettre en œuvre l'obligation de journalisation pour les traitements de données qui ne relèvent pas du champ d'application de la directive (UE) 2016/680, l'art. 46, al. 1, OPDo prévoit une période de transition de trois ans.

L'alinéa 3 prévoit désormais que, pour les données personnelles accessibles au public, il faut au moins journaliser l'enregistrement, la modification, l'effacement et la destruction des données. Cela signifie par exemple que la consultation de l'annuaire fédéral accessible au public ne doit pas obligatoirement être journalisée.

Un nouvel al. 4 vient compléter cette réglementation en explicitant concrètement la teneur de la journalisation. Ainsi, elle doit fournir des informations sur l'identité de la personne qui a effectué le traitement, la nature, la date et l'heure du traitement et, cas échéant, l'identité du destinataire des données.

L'al. 5 reprend la teneur de l'art. 10, al. 2, OLPD à quelques modifications près. Les procès-verbaux de journalisation devront être conservés durant un an au minimum, séparément du système dans lequel les données personnelles sont traitées. Cette durée minimale ne permet cependant pas de conserver les procès-verbaux de journalisation pendant une durée excessive. La durée de conservation doit en effet être proportionnée à la finalité de sécurité des

données. Par ailleurs, pour les organes fédéraux, le droit spécial est en tous les cas réservé. En particulier, l'ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération¹⁶ prévoit à son art. 4, al. 1, let. b, que les données résultant de l'utilisation de l'infrastructure électronique ne sont pas enregistrées plus que deux ans. La conservation séparée du système est nécessaire, car sinon le procès-verbal lui-même pourrait être manipulé ou chiffré en cas de cyberattaques. Les procès-verbaux sont uniquement accessibles aux organes ou personnes chargés de vérifier l'application des dispositions relatives à la protection des données personnelles ou de préserver ou restaurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, et ils ne seront utilisés qu'à cette fin. La notion de préservation vise à garantir que les administrateurs du système aient également accès aux procès-verbaux générés par le système s'ils soupçonnent une faille de sécurité. Ces données ne peuvent ainsi pas être utilisées dans un but de surveillance, notamment du comportement professionnel, des utilisateurs habilités. Une utilisation à des fins prévues par une loi spéciale, comme l'utilisation dans le cadre d'une procédure pénale, demeure bien entendu réservée.

La troisième phrase de l'art. 10, al. 1, OLPD, selon laquelle le préposé peut recommander la journalisation pour d'autres traitements, a été supprimée. Il serait contraire au système que le PFPDT puisse formuler des recommandations dans le domaine de la sécurité des données, qui fait l'objet d'une responsabilité pénale au sens de l'art. 61, let. c, nLPD. De plus, le PFPDT peut sans autre ordonner une journalisation dans le cadre de ses compétences décisionnelles générales, décrites à l'art. 51 nLPD, dans le contexte d'une enquête.

Art. 5 Règlement de traitement des personnes privées

L'obligation d'établir un règlement s'adressait au « maître du fichier automatisé soumis à déclaration », selon l'art. 11a, al. 3, LPD, qui ne peut se prévaloir des art. 11a, al. 5 b à d, pour ne pas déclarer ses fichiers (art. 11, al. 1, OLPD). Dans la mesure où l'obligation de déclarer les fichiers pour les responsables du traitement privés (art. 11a LPD) n'existe plus dans la nLPD, l'art. 11 OLPD ne peut être repris tel quel. Selon le principe de responsabilité ou d'« accountability » prévu par le RGPD, le responsable du traitement doit être en mesure de démontrer que les principes de traitement des données sont respectés (art. 5, par. 2 RGPD). Le droit suisse ne prévoit pas un devoir général de responsabilité ou « accountability », mais l'obligation d'établir un règlement du traitement remplit le même objectif.

L'obligation d'élaborer un règlement de traitement incombe au responsable du traitement et à son sous-traitant. L'art. 6 s'applique pour les sous-traitants privés qui agissent sur mandat des organes fédéraux. Si, exceptionnellement, un organe fédéral agit en tant que sous-traitant d'un responsable privé, il ne tomberait pas sous le coup de l'art. 5, qui ne couvre que les sous-traitants privés, mais de l'art. 6, qui est plus sévère. Cela se justifie de par la position et la responsabilité particulière qui incombent à l'organe fédéral en raison de sa nature juridique. Les règlements de traitement doivent être établis séparément.

Selon l'approche fondée sur le risque, il faut toujours établir un règlement de traitement lorsque le risque est élevé. Ainsi, les responsables du traitement privés doivent établir un règlement pour les traitements automatisés lorsqu'ils traitent des données sensibles à grande échelle (let. a) ou effectuent un profilage à risque élevé (let. b). La let. a correspond à la disposition de l'art. 22, al. 2, let. a, nLPD et porte sur le traitement de données sensibles à grande échelle. Elle exclut les cas où ces données sont traitées de façon isolée. Nombre

¹⁶ RS 172.010.442

d'entreprises, notamment des PME « traditionnelles », n'effectuent pas de tels traitements. Elles ne sont ainsi pas concernées par cette disposition.

L'al. 2 dresse la liste des indications que le règlement de traitement doit contenir au minimum. Les éléments de la liste reprennent, sous une forme parfois modifiée, et complètent les art. 11, al. 1 et 21, al. 2, OLPD. Comme dans le droit en vigueur, le règlement de traitement doit être conçu à la manière d'une documentation ou d'un manuel qui sert à la personne responsable¹⁷.

Comme c'est le cas actuellement, les responsables du traitement privés et leurs sous-traitants devront décrire l'organisation interne dans le règlement de traitement : cela comprend aussi une description de l'architecture et du fonctionnement des systèmes.

L'al. 2 dispose que les procédures de traitement des données, à savoir notamment les procédures d'enregistrement, de rectification, de communication, de conservation, d'archivage, de pseudonymisation, d'anonymisation, d'effacement ou de destruction des données, devront apparaître dans le règlement de traitement. Cela inclut les mesures prises pour la minimisation des données. Le principe de la minimisation des données est significatif pour la protection des données ; il découle, selon le message du 15 septembre 2017 sur la LPD¹⁸, du principe de la proportionnalité au sens de l'art. 6, al. 2, nLPD. Les procédures de traitement des données qui ont été mises en œuvre et les modalités de leur exécution devront y être décrites. Le règlement devra également décrire la procédure d'exercice du droit d'accès et du droit à la remise ou à la transmission des données personnelles. Les procédures de contrôles doivent permettre d'établir les autorisations d'accès, la nature et l'étendue de l'accès. Enfin, il est crucial que les mesures techniques et organisationnelles visant à garantir la sécurité adéquate des données figurent également dans le règlement de traitement. Le responsable et le sous-traitant devront indiquer les mesures qu'ils ont prises pour appliquer les objectifs de protection au sens de l'art. 2. Les indications devront aussi donner des renseignements sur la configuration des moyens informatiques, car ils constituent une mesure technique. L'ancien art. 21, al. 2, let. h, OLPD, qui mentionne expressément la configuration des moyens informatiques, n'a de ce fait pas été repris. Dans le règlement de traitement, il suffira de décrire les configurations de base des moyens informatiques ; il ne sera pas nécessaire d'entrer dans les détails techniques.

L'al. 3 reprend l'art. 11, al. 2, OLPD. En comparaison avec le droit en vigueur, on a renoncé à préciser que le règlement de traitement doit être mis à la disposition du conseiller sous une forme qui lui est intelligible. Le conseiller doit en toute logique pouvoir le comprendre puisqu'il participe lui-même à l'élaboration du règlement. L'obligation de mettre à disposition le règlement de traitement sur demande du préposé a été biffée. Le PFPDT pourra exiger l'accès au règlement dans le cadre d'une procédure d'enquête (art. 50, al. 1, let. a, nLPD), tout comme il pourra exiger l'accès au registre des activités de traitement.

Art. 6 Règlement de traitement des organes fédéraux

L'art. 6 correspond à l'art. 21 OLPD, sous réserve d'un certain nombre de modifications.

¹⁷ Voir commentaire OFJ, 6.1.4.

¹⁸ FF 2017 6565, 6644

L'obligation d'élaborer un règlement de traitement incombe à l'organe fédéral responsable et à son sous-traitant. Comme mentionné plus haut, l'art. 6 s'applique tant aux sous-traitants privés qu'aux organes fédéraux qui agissent exceptionnellement à titre de sous-traitant. Les règlements de traitement doivent être établis séparément.

Dans la phrase introductive de l'al. 1, on remplace les termes « fichiers automatisés » qui figurent à l'art. 21, al. 1, phrase introductive OLPD par « traitements automatisés ». Cette modification est nécessaire au motif que la nLPD ne recourt plus à la notion de « fichier ». Cette norme prévoit dorénavant que les organes fédéraux responsables établissent un règlement de traitement dans les cas énumérés aux let. a à f.

En raison de l'abrogation de la notion de « profil de la personnalité » et de l'introduction de la notion de « profilage » par la nLPD, il est nécessaire de modifier l'art. 21, al. 1, let. a, OLPD en prévoyant à l'art. 6, al. 1, OPDo que l'organe fédéral responsable et son sous-traitant sont tenus d'établir un règlement de traitement lorsqu'ils traitent des données sensibles (let. a), lorsqu'ils effectuent des profilages au sens de l'art. 5, let. f, nLPD (let. b) ou lorsqu'ils traitent des données au sens de l'art. 34, al. 2, let. c, nLPD (let. c). Le cas de figure de la let. a correspond au droit prévalant sous la LPD. En revanche, les let. b et c sont nouvelles. Elles remplacent l'obligation pour l'organe fédéral responsable d'établir un règlement de traitement pour tout fichier automatisé qui contient des profils de la personnalité (art. 21, al. 1, let. a, OLPD).

L'art. 6, al. 1, let. d OPDo ne subit que des modifications rédactionnelles par rapport à l'art. 21, al. 1, let. c OLPD.

Par rapport à l'art. 21, al. 1, let. d, OLPD, l'art. 6, al. 1, let. e est modifié en ce sens que le terme de « fichier » est supprimé et c'est l'expression « ensemble de données » qui est utilisée.

En vertu de l'art. 6, al. 1, let. f, OPDo un règlement de traitement doit également être établi lorsque l'organe fédéral responsable exploite un système d'information ou gère des ensembles de données conjointement avec d'autres organes fédéraux. Cette disposition remplace l'art. 21, al. 1, let. b, OLPD qui prévoit une telle obligation lorsqu'un fichier automatisé est utilisé par plusieurs organes fédéraux.

L'al. 2 reprend le contenu du règlement de traitement des personnes privées de l'art. 5, al. 2, OPDo. Il convient donc de se référer aux commentaires formulés précédemment.

L'al. 3 est une version légèrement retouchée de l'art. 21, al. 3, OLPD. Comme à l'art. 5, al. 3, OPDo, la précision que le règlement doit être mis à disposition sous une forme intelligible a été biffée. Le terme d'« organes chargés du contrôle » est remplacé par le conseiller à la protection des données. Il a été renoncé à mentionner le PFPDT pour les motifs expliqués ci-dessus en lien avec l'art. 5, al. 3, OPDo.

5.1.2 Section 2 : Sous-traitance

Art. 7

L'art. 7 OPDo règle la nature de l'autorisation préalable par laquelle un responsable du traitement peut autoriser un sous-traitant à confier le traitement de données à un tiers. Cette disposition s'appuie sur l'art. 22, par. 2 de la directive (UE) 2016/680 et l'art. 28, par. 2, RGPD.

Pour des raisons de sécurité juridique, elle reprend expressément ce que le Conseil fédéral avait déjà indiqué dans son message concernant la loi fédérale sur la protection des données au sujet de l'autorisation de la sous-traitance (voir FF 2017 6565, 6651). L'autorisation préalable du responsable du traitement peut être de nature spécifique ou générale (art. 7, al. 1, OPDo). En cas d'autorisation générale, le sous-traitant doit informer le responsable du traitement de tout changement envisagé en ce qui concerne le recours à d'autres tiers ou leur remplacement par un autre sous-traitant. Le responsable peut s'opposer à cette modification (art. 7, al. 2, OPDo).

5.1.3 Section 3 : Communication de données personnelles à l'étranger

Afin de suivre la systématique de la loi, les dispositions relatives à la communication de données personnelles à l'étranger sont intégrées dans le premier chapitre consacré aux dispositions générales. Plusieurs notions en lien avec la communication à l'étranger méritent d'être précisées. L'OPDo apporte ces précisions dans le cadre de cinq articles distincts : un premier article permet de concrétiser les critères à prendre en compte par le Conseil fédéral afin d'évaluer si un État, un territoire, un secteur déterminé dans un État, ou un organisme international garantit un niveau de protection adéquat ; un deuxième article prévoit de clarifier sur quoi doivent porter les clauses de protection des données d'un contrat et les garanties spécifiques assurant un niveau de protection approprié ; une troisième disposition traite des clauses types de protection des données ; un quatrième article se concentre sur les règles d'entreprise contraignantes. Enfin, sur la base de la compétence octroyée au Conseil fédéral par l'art. 16, al. 3, nLPD, une dernière disposition introduit d'autres garanties appropriées.

Art. 8 Évaluation du niveau de protection adéquat des données d'un État, d'un territoire, d'un secteur déterminé dans un État, ou d'un organisme international

Lorsque certains critères sont remplis, le Conseil fédéral peut considérer qu'un État ainsi qu'un territoire, un secteur déterminé dans un État ou un organisme international garantit un niveau de protection adéquat. Conformément à l'art. 7, al. 1, let. d, de l'ordonnance du 17 novembre 1999 sur l'organisation du Département fédéral de justice et police (Org DFJP)¹⁹, la tâche d'évaluer la garantie du niveau de protection adéquat d'un État, d'un territoire, d'un secteur déterminé dans un État, ou d'un organisme international fait partie des compétences dévolues à l'OFJ²⁰.

Il est prévu à l'art. 8, al. 1, OPDo que les États, les territoires, les secteurs déterminés dans un État ou les organismes internationaux – pour lesquels un niveau de protection adéquat a été constaté – soient mentionnés en annexe de l'ordonnance. Comme le préconise le message²¹, il s'agira dès lors d'une liste « positive ». Si un État n'y figure pas, cela ne signifie pas nécessairement qu'il est dépourvu d'une législation sur la protection des données assurant un niveau de protection adéquat ; il est possible qu'il n'ait simplement pas (encore) fait l'objet d'une évaluation par le Conseil fédéral. Toutefois, seuls les États qui figurent dans la liste du Conseil fédéral peuvent être considérés comme garantissant un niveau de protection adéquat. Ce procédé diffère quelque peu de celui appliqué par le PFPDT. En effet, jusqu'ici, le PFPDT a précisé pour chaque État si celui-ci a atteint un niveau adéquat, un niveau adéquat sous certaines conditions ou si le niveau est insuffisant ; il sied également de préciser que la

¹⁹ RS 172.213.1

²⁰ FF 2017 6565, 6791

²¹ FF 2017 6657

liste établie par le PFPDT n'a pas de valeur contraignante et ne lie notamment pas les tribunaux en cas de litige²². Avant de détailler les facteurs dont devra tenir compte le Conseil fédéral pour l'évaluation, il convient de préciser dans un premier temps ce qu'on entend par « territoire » ou « secteur déterminé dans un État ». La notion de « territoire » fait référence aux situations où l'ensemble d'un pays peut ne pas être soumis à une législation unique. Il en va particulièrement ainsi dans les États fédéraux, notamment lorsque l'État fédéral ne dispose pas d'une législation assurant un niveau de protection adéquat, alors qu'un État fédéré est en revanche doté d'un régime de protection des données adéquat, mais uniquement valable sur son propre territoire. Pour la notion de « secteur déterminé dans un État », on peut par exemple citer la liste du PFPDT qui tient compte, pour le Canada, du fait qu'une législation de protection spécifique pour le secteur privé ne permet de reconnaître un niveau de protection adéquat qu'à ce secteur²³. Jusqu'en juillet 2020, il en allait de même pour les États-Unis, en raison du *Privacy Shield CH-US* qui permettait le libre transfert des données uniquement vers les entreprises qui s'étaient engagées à respecter les principes contraignants du bouclier de protection des données²⁴. D'autres secteurs particuliers tels que le secteur financier, le secteur des assurances ou le secteur de la sous-traitance des traitements de données peuvent également être mentionnés²⁵. La notion d'organisme international était précisée dans le message relatif à la loi sur la protection des données. Il s'agit de « toute institution internationale, que ce soit une organisation ou une juridiction » (FF 2017 6565, 6657)²⁶.

Pour décider qu'un État, un territoire, un secteur déterminé dans un État, ou un organisme international assure un niveau de protection adéquat, les critères suivants doivent notamment être pris en compte (art. 8, al. 2 OPDo) :

- Les engagements internationaux de l'État ou de l'organisme international en matière de protection des données (al. 2, let. a) ; on pense ici en particulier à la Convention 108+²⁷, mais les engagements en matière de protection des données ne sont pas nécessairement les seuls pertinents, d'où l'usage de « notamment » (voir également le commentaire de la lettre c). Les accords réglant l'échange d'informations jouent également un rôle par exemple.
- L'état de droit et le respect des droits humains (al. 2, let. b) : la lettre b utilise la notion de « droits de l'homme » afin d'user de la même terminologie que celle de la CEDH et du Pacte ONU II. Le Conseil fédéral dispose d'une marge de manœuvre qui lui permet de constater qu'un État garantit un niveau de protection adéquat s'il adhère aux droits de l'homme reconnus internationalement dans son cadre juridique global, notamment s'agissant de la protection contre toute ingérence disproportionnée dans la vie privée, ceci quand bien même cet État ne remplirait pas en tous points les critères de la CEDH par exemple.

²² Cf. Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, p. 450 s.

²³ Cf. https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2020/staatenliste.pdf.download.pdf/20200908_Staatenliste_f.pdf. Dans le même sens, voir également la décision d'adéquation de la Commission européenne en faveur du Canada, qui reconnaît que la législation spécifique au secteur privé garantit un niveau de protection adéquat : Décision 2002/2/CE de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, J.O.C.E., L 2 du 4 janvier 2002.

²⁴ Nachdem der EuGH am 16. Juli 2020 den Privacy Shield EU-USA für ungültig erklärt hatte (Urteil «Schrems II»), hat der EDÖB in seiner Staatenliste den Verweis auf einen « angemessenen Datenschutz unter bestimmten Bedingungen » für die USA gestrichen. Siehe dazu die Medienmitteilung des EDÖB (<https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-80318.html>) und seine Stellungnahme (<https://www.news.admin.ch/newsd/message/attachments/64258.pdf>).

²⁵ Cf. De Terwangne Cécile/Gayrel Claire, Le RGPD et les transferts internationaux de données à caractère personnel, in : Le règlement général sur la protection des données (RGPD/GDPR): analyse approfondie, Cahiers du CRIDS; No. 44, 2018, <http://www.crid.be/pdf/public/8344.pdf>, p. 297.

²⁶ Les autres précitées mentionnent par exemple l'Agence Mondiale Anti-dopage, à Montréal, vers laquelle des données sensibles sur la santé des sportifs de haut niveau sont transférées. De Terwangne Cécile/Gayrel Claire, p. 296.

²⁷ Protocole d'amendement à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE n° 223.

- La législation applicable, notamment en matière de protection des données, de même que sa mise en œuvre et la jurisprudence y relative (al. 2, let. c) : le « notamment » appuie une formulation comprenant la législation sectorielle. Celle-ci abonde très souvent en dispositions (directes et/ou indirectes) relatives à la protection des données. Il en va par exemple ainsi des États qui ne disposeraient pas d'une législation cadre en matière de protection des données, mais uniquement d'un Code civil. Dans certains cas, ces États ont des lois sectorielles contenant des articles relatifs à la protection des données. Il s'agit de pouvoir s'en remettre aux lois applicables. Partant, l'accent est mis sur la législation pertinente de l'État, tant générale que spéciale, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale, le droit pénal ainsi qu'en ce qui concerne l'accès des autorités publiques aux données personnelles.
- La garantie effective des droits des personnes concernées et des voies de droit (al. 2, let. d) ; il ne s'agit pas seulement de vérifier si les droits des personnes concernées figurent dans des bases légales, mais bien de s'assurer que ces droits sont effectivement mis en œuvre.
- Le fonctionnement effectif d'une ou de plusieurs autorités indépendantes chargées de la protection des données dans l'État concerné, ou auxquelles un organisme international est soumis, et disposant de pouvoirs et de compétences suffisants. Dans ce sens, les exigences minimales de la Convention 108+ doivent être remplies (al. 2, let. e).

Le troisième alinéa précise que le PFPDT est consulté lors de toute évaluation portant sur l'adéquation. Son avis ne lie pas le Conseil fédéral, mais il doit être pris en compte, notamment dans le cadre de la procédure de consultation des offices. Le PFPDT peut, en outre publier son avis. Par ailleurs, le Conseil fédéral peut aussi tenir compte de l'existence d'une évaluation relative au niveau de protection effectuée soit par une autorité étrangère chargée de la protection des données (qui provient d'un État assurant un niveau de protection adéquat), soit par un organisme international. Par organisme international, au sens de cet alinéa, on peut notamment entendre le Comité conventionnel institué par la Convention STE 108. Les évaluations effectuées par la Commission européenne peuvent également constituer une source d'information.

Le quatrième alinéa prévoit que le niveau de protection dans l'État ou l'organisme concerné est réévalué périodiquement.

Suite aux différentes prises de position exprimées lors de la consultation externe, un nouvel al. 5 prévoit que les évaluations effectuées par l'OFJ sont publiées. La notion d'évaluation comprend autant l'évaluation que la réévaluation d'un État, d'un territoire, d'un secteur déterminé dans un État ou d'un organisme international, qui était déjà dans la liste et qui est évalué une nouvelle fois. Une disposition transitoire (art. 46, al. 2) est introduite afin de préciser que les évaluations effectuées avant l'entrée en vigueur de l'OPDo ne seront pas rendues publiques.

L'ordonnance introduit une pesée d'intérêts permettant d'agir dans l'urgence lorsqu'il est possible de conclure que le niveau d'adéquation n'est plus garanti. L'al. 6 déclare que s'il est constaté que le niveau de protection n'est plus garanti par un État, un territoire, un secteur déterminé dans un État ou un organisme international, l'annexe 1 est modifiée. Par exemple, dans le cas des États-Unis, l'arrêt « Schrems II » rendu par la CJUE en juillet 2020 a conduit le PFPDT à revoir sa position et à modifier sa liste. Si des informations permettent de constater qu'un État concerné ne garantit plus un niveau de protection adéquat (p. ex. une crise po-

litique), le Conseil fédéral peut modifier la liste de manière urgente sans attendre d'avoir effectué un examen formel et complet. En effet, l'art. 7, al. 3, LPubl²⁸ permet les publications urgentes. Il est souligné que cela s'applique uniquement dans le cas d'un éventuel retrait. Tout ajout dans la liste doit respecter le processus d'évaluation (al. 1 et 2). La modification n'a pas d'effet sur les communications des données déjà effectuées.

Art. 9 Clauses de protection des données d'un contrat et garanties spécifiques

L'art. 16, al. 2, nLPD prescrit que des données personnelles peuvent être communiquées vers un État qui ne figure pas à l'annexe 1 de l'ordonnance, soit en l'absence d'une évaluation du niveau de protection adéquat par le Conseil fédéral, pour autant qu'un niveau de protection approprié soit garanti. Dans le secteur privé, cette garantie peut être fournie par des clauses de protection des données d'un contrat entre le responsable du traitement ou le sous-traitant et son co-contractant (art. 16, al. 2, let. b, nLPD). Dans le secteur public, il peut s'agir de garanties spécifiques élaborées par l'organe fédéral compétent (art. 16, al. 2, let. c, nLPD).

Contrairement aux autres instruments prévus à l'al. 2 de l'art. 16 nLPD, les responsables du traitement et les sous-traitants ne doivent pas faire approuver ces garanties par le PFPDT, mais uniquement les lui communiquer avant toute transmission de données personnelles à l'étranger. Il existe un certain risque que les responsables du traitement et les sous-traitants aient une interprétation différente concernant le degré de protection que ces garanties doivent atteindre, ceci aussi bien dans leur secteur privé que dans le secteur public.

Le Conseil fédéral considère par conséquent qu'il est opportun de définir certains standards de protection des données et précise à l'art. 9, al. 1, OPDo ce que ces clauses de protection des données ou garanties spécifiques doivent régler au minimum.

Il s'agit en particulier des éléments suivants :

- L'application des principes de licéité, de bonne foi, de proportionnalité, de transparence, de finalité et d'exactitude (let. a).
- Les catégories de données communiquées et de personnes concernées (let. b).
- Le type et la finalité de la communication des données personnelles (let. c).
- Le cas échéant, le nom des États ou des organismes internationaux auxquels sont destinées les données personnelles, et les conditions applicables à la communication (let. d) : l'usage de l'expression « le cas échéant » permet de s'adapter aux circonstances du contrat. Dans le cas de certains contrats très délimités, cette lettre peut ne pas entrer en considération. À titre d'exemple si, dans le cadre du contrat, aucune donnée n'est transmise à un organisme international, une telle mention n'a évidemment pas lieu d'être.
- Les conditions applicables à la conservation, à l'effacement et la destruction des données personnelles (let. e).
- Les destinataires ou catégories de destinataires (let. f) : les catégories de destinataires peuvent apparaître utiles ne serait-ce que de façon générique lorsque cela s'impose (par exemple : des représentants, des sous-traitants, des co-responsables, des médecins traitants, des communes, des organismes externes partenaires, etc.).
- Les mesures visant à garantir la sécurité des données (let. g).
- L'obligation d'annoncer les violations de la sécurité des données (let. h).

²⁸ RS 170.512

- L'obligation pour le responsable du traitement destinataire d'informer les personnes concernées par le traitement des données (let. i) : le destinataire sous-traitant ne peut pas être responsable et répondre à cette obligation.
- Les droits de la personne concernée (let. j), en particulier : le droit d'accès et le droit à la remise ou à la transmission des données personnelles (ch. 1), le droit de s'opposer à la communication des données (ch. 2), le droit de demander la rectification, l'effacement ou la destruction de données (ch. 3) et le droit de saisir en justice une autorité indépendante (autorité de protection des données ou tribunal) (ch. 4).

Tous ces éléments reprennent les fondements de la nLPD et un al. 2 vient encore préciser que lorsqu'il communique des données personnelles à l'étranger, le responsable du traitement prend les mesures adéquates pour s'assurer que le destinataire respecte les clauses de protection des données du contrat ou les garanties spécifiques ; le sous-traitant devra en faire de même s'agissant des clauses de protection des données du contrat (le mécanisme de sous-traitance ne s'applique pas aux garanties spécifiques). Cet alinéa (qui reprend pour l'essentiel l'art. 6, al. 2 et al. 4 OLPD) permet ainsi de s'assurer que le destinataire des données communiquées respecte le cadre de la protection des données applicable en Suisse.

Enfin, un troisième alinéa reprend l'al. 2 de l'art. 6 OLPD concernant le devoir d'information du responsable du traitement. Il n'est modifié que de manière formelle (par exemple dans la version française, le terme « maître du fichier » est remplacé), la deuxième partie de la phrase de l'art. 6, al. 2, let. b, OLPD étant supprimée. Une communication à l'étranger n'est de toute façon autorisée que si les clauses de protection des données ou les garanties assurent un niveau de protection suffisant dans la mesure où elles remplissent les conditions énoncées à l'art. 9, al. 1, OPDo. Il n'est par conséquent pas nécessaire de le mentionner à nouveau à l'art. 9, al. 3, let. b, OPDo.

Art. 10 Clauses types de protection des données

Comme dans le cadre de la communication de données à l'étranger fondée sur des clauses de protection des données d'un contrat et des garanties spécifiques, la communication qui repose sur des clauses types de protection des données (art. 16, al. 2, let. d, nLPD) doit respecter le droit suisse de la protection des données. Ainsi, l'art. 10, al. 1, OPDo, qui correspond à l'art. 6, al. 4, OLPD, précise que le responsable du traitement ou le sous-traitant doit prendre des mesures adéquates pour s'assurer que le destinataire respecte bien les clauses types. Le commentaire de l'OLPD rédigé par l'OFJ²⁹ décrit cette obligation de diligence de la manière suivante : « La question de savoir si les mesures sont adéquates dépend des circonstances du cas d'espèce. Les exigences seront plus élevées s'il s'agit de données sensibles ou de profils de la personnalité que pour les autres données personnelles ». Bien que la notion de « profils de la personnalité » n'existe plus dans la nLPD, l'explication n'en reste pas moins pertinente pour comprendre que les mesures adéquates doivent être adaptées aux circonstances concrètes. Il s'agit d'une obligation de moyen et le responsable du traitement, respectivement le sous-traitant, doit veiller à mettre en place ces mesures et à assurer le suivi de leur application.

L'al. 2 concerne l'approbation par le PFPDT des clauses types de protection des données élaborées par une personne privée ou par un organe fédéral. Le PFPDT rend une prise de position et publie, sur son site Internet, la liste des clauses types de protection des données qu'il a approuvées, établies ou reconnues. Partant, les clauses types doivent répondre aux

²⁹ Cf. Commentaire OFJ, 5.2.

exigences suisses en matière de protection des données et pouvoir être interprétées conformément à la législation suisse relative à la protection des données. Le PFPDT « communique le résultat de son examen sur les clauses types qui lui sont soumises dans un délai de 90 jours ».

Art. 11 Règles d'entreprise contraignantes

Les règles d'entreprise contraignantes s'appliquent à toutes les entreprises appartenant à un même groupe et doivent être respectées par celles-ci. Ces règles doivent non seulement porter sur les points mentionnés à l'art. 9, al. 1, OPDo, mais aussi sur la structure et les coordonnées du groupe d'entreprise et de chacune de ses entités (al. 2, let. a), ainsi que sur les mesures mis en place au sein des groupes d'entreprises pour garantir que ces règles d'entreprises soient effectivement respectées (al. 2, let. b).

Ces règles d'entreprise contraignantes doivent, conformément à l'art. 16, al. 2, let. e, nLPD, être soumises au PFPDT.

L'art. 11 OPDo comprend un nouvel al. 3 selon lequel « le PFPDT communique le résultat de son examen sur les règles d'entreprise contraignantes qui lui sont soumises dans un délai de 90 jours ».

Art. 12 Codes de conduite et certifications

Comme l'indique l'art. 16, al. 3, nLPD, le Conseil fédéral peut prévoir d'autres garanties appropriées permettant de communiquer des données à l'étranger. Peuvent ainsi assurer un niveau de protection approprié, un code de conduite ou une certification (al. 1).

Cette nouvelle mesure permet d'inciter les entreprises à adopter de tels codes ou à faire certifier leurs systèmes, produits ou services. Par souci de cohérence avec les clauses types de protection des données et les règles d'entreprise contraignantes qui doivent être approuvées par le PFPDT, il en va de même pour ces codes de conduite (al. 2). Il convient en effet de faire vérifier la solidité de ces instruments. Pour son examen, le PFPDT peut s'inspirer des critères de l'art. 9, al. 1, OPDo. L'approbation des codes de conduite par le PFPDT n'entre pas en contradiction avec l'art. 11 nLPD qui prévoit que, de manière générale, le PFPDT prend position sur les codes de conduite qui lui sont soumis (et ne les approuve pas). Dans le cas précis où un responsable du traitement entend se prévaloir de son code de conduite pour communiquer des données personnelles à l'étranger, il est cohérent, par rapport aux clauses types de protection des données et aux règles d'entreprises contraignantes, que le PFPDT approuve cet instrument. Conformément à l'ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données³⁰, seules les certifications étrangères doivent être reconnues par le PFPDT. Cette situation est maintenue dans l'ordonnance entièrement révisée. Cela n'empêche cependant pas que la certification doive être conforme aux exigences de l'ordonnance sur les certifications en matière de protection des données.

De surcroît, le responsable du traitement ou le sous-traitant qui se situe dans un pays tiers doit prendre l'engagement contraignant et exécutoire d'appliquer les mesures contenues dans les codes de conduite ou les certifications (al. 3).

³⁰ RS 235.13

Suppression des art. 5 et 7 OLPD

Il convient encore de mentionner que les art. 5 et 7 OLPD ne sont pas repris : le premier a désormais été intégré au niveau de la nLPD (art. 18) et le second, qui donnait au PFPDT la compétence d'édicter une liste des États ayant un niveau de protection adéquat, n'est plus pertinent, puisque cette compétence revient désormais au Conseil fédéral (art. 16, al. 1, nLPD).

5.2 Chapitre 2 : Obligations du responsable du traitement

Art. 13 Modalités du devoir d'informer

Le devoir d'informer du responsable du traitement est ancré à l'art. 19 nLPD. Il est accompagné d'exceptions et de restrictions inscrites à l'art. 20 nLPD. À l'art. 19 al. 1, nLPD, il est spécifié que la personne concernée doit être informée « de manière adéquate ». Cela implique que les informations soient communiquées si possible de manière concise, transparente, compréhensible et aisément accessible.

En d'autres termes, cela signifie que le responsable du traitement doit s'assurer, lors du choix des modalités d'informations, que les informations les plus importantes sont toujours transmises dans le premier niveau de communication avec la personne concernée lors de la collecte de ses données personnelles. Par exemple, lorsque la communication se fait sur un site internet, une bonne pratique peut consister à faire en sorte que les informations essentielles soient toutes disponibles en un coup d'œil, par exemple sous la forme d'un aperçu. Pour obtenir des informations complémentaires, la personne concernée pourra ensuite cliquer sur ces premières informations et cela ouvrira une autre fenêtre contenant des détails supplémentaires. Il faut néanmoins préciser que la communication par un site internet n'est pas toujours suffisante : il faut que la personne concernée sache qu'elle trouvera ces informations sur un site en particulier. Dans le cas d'un entretien téléphonique, des explications orales peuvent aussi être fournies, lesquelles peuvent être complétées par un renvoi vers un site internet ; s'il s'agit d'informations enregistrées, la personne concernée devra avoir la possibilité d'entendre des informations plus détaillées. Enfin, dans le cas où la personne est filmée par un système de vidéosurveillance fixe ou par un drone, un panneau indicateur ou une campagne d'information devront par exemple mentionner cette activité.

Conformément à l'art. 19, al. 1, nLPD, l'art. 13 OPDo s'applique uniquement au responsable du traitement mais pas au sous-traitant. Il convient toutefois de préciser que, conformément à l'art. 19, al. 2, let. c, nLPD, la communication du responsable du traitement doit également contenir des informations relatives aux destinataires ou aux catégories de destinataires auxquels des données personnelles sont transmises. Selon les explications du message concernant la loi sur la protection des données, les sous-traitants font partie des destinataires (FF 2017 6565, 6669). Le responsable doit donc également informer la personne concernée que les données seront communiquées à un sous-traitant.

Art. 14 Conservation de l'analyse d'impact relative à la protection des données personnelles

La disposition précise la durée de conservation de l'analyse d'impact relative à la protection des données personnelles au sens de l'art. 22 nLPD. Elle devra être conservée pendant deux ans au moins. Si l'analyse d'impact relative à la protection des données doit être conservée après que le traitement des données ait eu lieu, c'est parce qu'elle constitue un instrument central de la législation sur la protection des données. Elle peut notamment se révéler importante lorsqu'il faut faire la lumière sur une violation de la sécurité des données ou évaluer

la punissabilité d'un comportement. Elle fournit donc des informations sur la façon dont on a évalué les risques pour la personnalité et les droits fondamentaux, et les mesures qui ont été prises. Dans le cas des organes fédéraux qui, en principe, ne peuvent traiter des données que s'il existe une base légale, il peut arriver qu'en raison de certaines bases légales existant depuis longtemps, une analyse d'impact relative à la protection des données doive être conservée pendant une très longue période.

Dans le cas des organes fédéraux, il sera également nécessaire de réglementer la manière dont l'analyse d'impact relative à la protection des données doit être coordonnée avec la procédure législative de création de la base légale pour le traitement des données. Il convient de prévoir que les organes fédéraux doivent inclure l'analyse d'impact relative à la protection des données avec les projets d'actes législatifs dans la proposition au Conseil fédéral et qu'ils doivent intégrer les résultats de l'analyse au message du Conseil fédéral. Toutefois, étant donné que la réglementation n'a que le caractère d'une directive interne à l'administration fédérale, elle ne doit pas être réglée au niveau de l'ordonnance. Il est prévu de mettre en œuvre ces règles dans les directives sur les affaires du Conseil fédéral (« classeur rouge ») et dans l'aide-mémoire sur la présentation des messages du Conseil fédéral.

Le PFPDT pourra utiliser ses compétences et élaborer des outils valant recommandations de bonne pratique au sens de l'art. 58, al. 1, let. g, nLPD. Pour ce faire, il dispose d'une certaine marge de manœuvre.

Art. 15 Annonce des violations de la sécurité des données

L'art. 24, al. 2, nLPD spécifie les indications minimales que le responsable du traitement doit communiquer lors de l'annonce d'une violation de la sécurité des données au PFPDT : la nature de cette violation, ses conséquences et les mesures prises ou envisagées. L'art. 15, al. 1, OPDo (précédemment l'art. 19, al. 1, P-OLPD) précise plus en détail le contenu de cette annonce. Il convient de relever que l'annonce au PFPDT au sens de l'art. 24, al. 1, nLPD se limite aux violations de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Seules les violations de la sécurité des données qu'il est obligatoire de déclarer devront être annoncées.

L'al. 1 comporte un catalogue d'informations : outre la nature de la violation des données, déjà mentionnée dans la loi (let. a), il faudra communiquer, dans la mesure du possible, le moment et la durée de la violation (let. b). Le responsable devra aussi communiquer dans la mesure du possible les catégories et le nombre approximatif de données personnelles concernées (let. c), ainsi que les catégories et le nombre approximatif de personnes concernées (let. d). Ces informations sont cruciales pour estimer la gravité de la violation. Le PFPDT a en particulier besoin de savoir quelles catégories de données personnelles sont concernées (p. ex. adresses, informations relatives aux cartes de crédit, données concernant la santé) pour comprendre les conséquences et les risques pour les personnes concernées (let. e) et les mesures prises ou envisagées (let. f) qui lui sont communiquées par le responsable du traitement. Cela permet à la personne concernée de prendre elle-même des mesures concrètes (p. ex. changement immédiat de mot de passe si des données de connexion ont été volées, ou blocage de la carte). Enfin, le responsable du traitement devra fournir le nom et les coordonnées d'une personne de contact (let. g) pour la communication avec le PFPDT et la personne concernée.

L'al. 2 permet au responsable du traitement de fournir progressivement les informations au PFPDT s'il n'est pas en mesure de lui fournir toutes les informations visées à l'al. 1 au moment où une violation de la sécurité des données est détectée. D'après l'art. 24, al. 1,

nLPD, le responsable doit annoncer ces violations « dans les meilleurs délais ». Toutefois, en pratique, les informations au sens de l'al. 1, let. b à d, ne sont souvent pas disponibles immédiatement après la détection de la violation. L'al. 2 permettra donc au responsable du traitement de ne fournir que les informations dont il dispose dans un premier temps. Dès qu'il disposera des autres informations, qu'il doit tâcher de réunir sans retard injustifié, il les transmettra au PFPDT au fur et à mesure. Pour les annonces fournies a posteriori, la règle est que le responsable du traitement doit faire l'annonce « dans les meilleurs délais », comme cela figure à l'art. 24, al. 1, nLPD. Dès qu'il dispose des informations manquantes, le responsable doit les mettre à disposition du PFPDT en les communiquant a posteriori. S'il doit encore obtenir des informations, il doit s'en occuper sans plus attendre.

L'al. 3 indique les informations qui doivent être communiquées à la personne concernée à informer en application de l'art. 24, al. 4, nLPD. Il est par ailleurs précisé que cette communication devra se faire dans un langage simple et compréhensible, ce qui n'est pas nécessairement le cas de l'annonce au PFPDT. En effet, il ne faut pas supposer qu'une personne ordinaire connaisse le jargon de cette matière technique. Le contenu de l'annonce au PFPDT est décrit de façon plus extensive car celui-ci doit pouvoir se faire une idée de l'ampleur de la violation de la sécurité des données.

L'al. 4 prescrit qu'il faut documenter les faits relatifs aux violations de la sécurité des données, leurs effets ainsi que les mesures prises. Les documents devront être conservés pendant au moins deux ans à compter de la date à laquelle la violation est annoncée.

Dans le contexte de la mise en œuvre de l'obligation d'annoncer de l'art. 24 nLPD, ajoutons qu'il faudra s'attendre à ce que le PFPDT reçoive un grand nombre d'annonces chaque année : c'est ce qui ressort de l'expérience des autorités de surveillance étrangères depuis que l'obligation de notification, semblable à la nôtre, inscrite à l'art. 33 du règlement (UE) 2016/679 est entrée en vigueur. Des échanges avec l'office de la protection des données de la Bavière ont permis d'estimer qu'environ 6000 annonces pourraient être faites chaque année en rapportant les chiffres enregistrés à la Suisse. Le PFPDT se penche actuellement sur le développement d'une interface web pour les annonces, qui devrait revêtir la forme d'un formulaire interactif afin de structurer les annonces et d'assurer un traitement efficace du grand nombre d'annonces à venir. Dans le cadre de ce projet, il étudie la possibilité de créer un portail d'annonce en commun avec les autres organes fédéraux qui prévoient aussi des possibilités de ce type pour les annonces de violation de la sécurité des données (p. ex. l'annonce au sujet des infrastructures critiques). Un portail commun permettrait de réduire la charge de travail des responsables du traitement, surtout s'ils doivent soumettre des annonces à plusieurs services de la Confédération.

5.3 Chapitre 3 : Droits de la personne concernée

Le chapitre relatif aux droits de la personne concernée traitait, dans le cadre du P-LPD, du droit d'accès et des restrictions à ce droit. Le Parlement a cependant décidé d'y ajouter un droit à la remise et à la transmission des données personnelles. L'ordonnance vient donc préciser ces volets des droits de la personne concernée dans deux sections distinctes.

La première section traite du droit d'accès. Après discussion avec le Département fédéral des affaires étrangères et celui de la défense, de la protection de la population et des sports, le contenu de l'art. 14 OLPD n'a pas été repris dans l'OPDo parce qu'il n'est plus d'actualité. Il a donc été décidé de régler le droit d'accès pour les deux secteurs (privé et public) dans une partie commune qui suit la structure de la nLPD et s'inscrit à la suite des obligations des responsables du traitement.

Désormais, les différents éléments relatifs au droit d'accès se répartissent sur plusieurs articles. Un premier article se concentre sur les modalités du droit d'accès et en particulier sur la forme de la communication des renseignements ; un deuxième article est consacré au droit d'accès lorsque plusieurs responsables du traitement traitent en commun des données personnelles ou que des données sont sous-traitées ; un troisième article traite des délais applicables ; enfin, un quatrième article règle les exceptions à la gratuité du droit d'accès.

La deuxième section concerne le droit à la remise ou à la transmission des données personnelles. Elle comporte les articles suivants : l'art. 20, qui porte sur l'étendue du droit ; l'art. 21, concerne les exigences techniques de mise en œuvre, et l'art. 22 (ancien art. 24 P-OLPD) précise qu'en matière de délais, de modalités et de responsabilité, les dispositions relatives au droit d'accès s'appliquent par analogie.

5.3.1 Section 1 : Droit d'accès

Art. 16 Modalités

Cette disposition concrétise les modalités du droit d'accès prévu à l'art. 25 nLPD. Elle reprend, dans une certaine mesure, l'art. 8, al. 5, LPD et l'art. 1, al. 1 à 3, OLPD.

Al. 1

L'art. 16 OPDo (ancien art. 20 P-OLPD) se concentre, à l'al. 1, sur la forme que doit prendre la demande d'accès. La forme écrite au sens de l'art. 16, al. 1, OPDo comprend toutes les formes qui permettent d'établir la preuve par le texte. On ne parle pas ici de la forme écrite simple au sens des art. 13 à 15 du code des obligations (CO)³¹. Celle-ci requiert une signature manuscrite ou une signature électronique qualifiée avec horodatage électronique qualifié, conformément à la loi du 18 mars 2016 sur la signature électronique³². L'art. 16, al. 1, OPDo exige uniquement la présence d'un texte écrit. En substance, il reprend le contenu de l'art. 1, al. 1, OLPD qui prescrit que la personne qui fait valoir son droit d'accès « doit en règle générale le faire par écrit ». Le commentaire de l'OLPD rédigé par l'OFJ³³ précise déjà que la forme orale peut suffire dans certains cas et pour autant que le maître de fichier (désormais le responsable du traitement) soit d'accord. L'art. 16 OPDo a donc été remanié dans ce sens, privilégiant ainsi une plus grande clarté. Par ailleurs, l'art. 1, al. 1, OLPD a été repris avec des adaptations sur le plan rédactionnel.

Al. 2

A l'inverse du droit en vigueur, l'art. 16, al. 2, OPDo (ancien art. 20, al. 2, P-OLPD) dispose explicitement que les renseignements peuvent aussi être fournis sous la forme dans laquelle les données se présentent, en plus de la forme écrite. En règle générale, les données personnelles revêtent la forme écrite. En revanche, si les données sont des images ou des enregistrements audio, la personne concernée les recevra dans leur forme originale. Comme expliqué ci-dessus, le critère de la forme écrite signifie ici que l'on exige un texte écrit.

Comme prévu à l'art. 1, al. 3, OLPD, la consultation sur place est par exemple possible, notamment lorsque les données sont réparties dans différents dossiers, qu'elles ont une am-

³¹ RS 220

³² RS 943.03

³³ Cf. Commentaire OFJ, 3.1.

pleur particulière ou que des explications doivent accompagner les renseignements demandés. À la différence de l'art. 1, al. 3, OLPD, le passage concernant le fait que la consultation sur place doit se faire sur proposition du maître du fichier a été biffé. Il reste nécessaire que le responsable et la personne concernée se soient entendus sur le sujet, peu importe de savoir de qui la proposition de la consultation sur place émane. En cas de consultation sur place, la personne concernée doit néanmoins avoir la possibilité de demander une photocopie de certaines pièces de son dossier. Comme le Tribunal fédéral l'a indiqué dans l'ATF 119 III 141, la délivrance de documents écrits (y compris électroniques) peut être extrêmement importante pour la personne concernée. La transmission des informations par oral, par exemple par téléphone, est également prévue, pour autant que la personne concernée y ait consenti. Enfin, les renseignements sous forme résumée (agrégée) ne sont pas autorisés.

Al. 3

L'al. 3 reprend, sous une forme modifiée, l'art. 1, al. 2, OLPD. Il règle la façon dont la demande de renseignement et la communication des renseignements peuvent être effectuées : la voie électronique est autorisée. La personne concernée peut par exemple adresser sa demande à une entreprise par courriel ou via une plateforme en ligne (p. ex. via les comptes clients, qui sont de plus en plus répandus). Conformément aux règles en vigueur, il incombe à l'expéditeur de prouver que son message a atteint le destinataire. L'al. 3 est une disposition déclaratoire puisque la transmission par voie électronique est autorisée sans qu'une base légale ne soit nécessaire.

Al. 4

Lorsque les données personnelles sont fournies dans un format « technique », qui n'est pas lisible et/ou compréhensible pour la personne concernée, le responsable du traitement doit être en mesure de lui donner des explications complémentaires, par exemple oralement.

Al. 5

Le responsable du traitement doit prendre les mesures adéquates pour assurer l'identification de la personne concernée, raison pour laquelle celle-ci doit coopérer à son identification. Afin que le responsable puisse s'assurer de l'identification, il a besoin que la personne concernée lui fournisse les informations nécessaires. Si cela se fait par oral, le responsable s'assurera au préalable (par exemple en demandant le numéro AVS) qu'il fournit les renseignements à la bonne personne. L'art. 15, al. 5, OPDo (ancien art. 20, al. 4, P-OLPD) remplace l'exigence fixée à l'art. 1, al. 1, OLPD d'après laquelle la personne concernée doit justifier de son identité.

Autres éléments

En ce qui concerne l'al. 4 de l'article 1 OLPD, consacré à la question du délai pour fournir des renseignements, il fait désormais l'objet d'un article spécifique (voir art. 18 OPDo, ancien art. 22 P-OLPD, ci-dessous). Il en va de même pour les al. 5 et 6 de l'art. 1 OLPD (voir art. 17 OPDo, ancien art. 21 P-OLPD, ci-dessous).

Art. 17 Responsabilité

Un article distinct est prévu pour préciser les compétences dans les cas où plusieurs responsables du traitement traitent en commun des données personnelles.

Al. 1

Le premier alinéa reprend l'al. 5 de l'art. 1 OLPD, sous une forme adaptée. Du point de vue terminologique, la notion de maître du fichier est remplacée par celle de responsable. L'exception à la possibilité de faire valoir le droit d'accès auprès de chaque responsable du traitement est supprimée. Cela signifie que la personne concernée peut toujours exercer son droit d'accès auprès de chaque responsable du traitement. Contrairement à l'art. 1, al. 5, OLPD, l'art. 17, al. 1, OPDo n'exige plus que les responsables transmettent la requête, au contraire, ils devront fournir des renseignements dans tous les cas. Cet alinéa correspond à l'art. 21, par. 2 de la directive (UE) 2016/680 et à l'art. 26, par. 3, RGPD.

Al. 2

Le deuxième alinéa reprend l'al. 6 de l'art. 1 OLPD sous une forme adaptée. La notion de sous-traitant introduite dans la nLPD (art. 5, let. k, nLPD) est reprise et la notion de maître du fichier est remplacée par celle de responsable du traitement. Selon l'art. 25, al. 4, nLPD, le responsable demeure tenu de fournir les renseignements demandés même s'il fait traiter des données personnelles par un sous-traitant. Celui-ci n'a donc pas d'obligation légale de répondre lui-même aux demandes de renseignements. L'art. 17, al. 2, OPDo prévoit, contrairement à l'OLPD, que le sous-traitant aide le responsable pour autant qu'il ne réponde pas lui-même à la demande pour le compte du responsable du traitement. Cela signifie que le sous-traitant devra fournir au responsable les données dont il ne dispose pas encore.

Art. 18 Délais

L'art. 18 OPDo (ancien art. 22 P-OLPD) reprend sans modification substantielle le quatrième alinéa de l'art. 1 OLPD et vient ainsi préciser l'al. 7, introduit à l'art. 25 nLPD par le Parlement, et qui remonte au niveau de la loi le délai de 30 jours prévu jusqu'alors dans l'ordonnance. La précision selon laquelle une décision restreignant le droit d'accès doit être motivée a été supprimée dans la mesure où cette norme est déjà inscrite à l'art. 26, al. 4, nLPD. Enfin, le terme de « requérant » est remplacé par celui de « personne concernée » afin d'avoir une unité terminologique avec la nLPD.

En substance, cette norme signifie que le responsable du traitement dispose de 30 jours pour donner les renseignements demandés par la personne concernée ou lui indiquer qu'il refuse, restreint ou diffère le droit d'accès. Dans le domaine public, communiquer des renseignements, refuser, restreindre ou différer la communication de renseignements équivaut à une décision au sens de l'art. 5 de la loi fédérale du 20 décembre 1968 sur la procédure administrative (PA)³⁴. L'al. 2 ne trouve application que si le responsable du traitement n'est pas en mesure de donner les renseignements dans les 30 jours suivant la réception de la demande (et pas dans le cas où il restreint le droit d'accès au sens de l'art. 26 nLPD) : le responsable du traitement est tenu d'indiquer à temps, sans retard injustifié, dans quel délai les renseignements seront fournis.

Art. 19 Exception à la gratuité

Le titre de la disposition subit une modification rédactionnelle par rapport à l'art. 2 OLPD.

³⁴ RS 172.021

Al. 1

L'art. 2, al. 1, let. a, OLPD, qui concerne les cas dans lesquels les demandes d'accès sont procéduriales, est supprimé. Ce cas de figure est désormais réglé dans la nLPD, qui prévoit à son art. 26, al. 1, let. c, que le responsable du traitement peut refuser, restreindre ou différer la communication des renseignements lorsque la demande d'accès est manifestement procédurale.

L'art. 2, al. 1, let. b et al. 2 OLPD est repris moyennant quelques modifications. Le terme « exceptionnellement » est supprimé dans la mesure où l'intitulé de l'article parle déjà d'« exception » et le terme « requérant » (nouvel al. 3) est remplacé par celui de « personne concernée » dans un souci d'uniformité avec la nLPD. La notion de « volume de travail considérable » est remplacée par celle d'« efforts disproportionnés » afin de garder une cohérence avec les modifications introduites par le Conseil national à l'art. 25, al. 6 nLPD. À titre d'exemple, le cas dans lequel le responsable du traitement doit donner accès à de nombreuses données personnelles parce qu'il a précisément un intérêt à collecter le plus de données possible ne constitue pas un effort disproportionné. Il en va de même lorsque le travail est considérable parce que le responsable du traitement a une organisation insuffisamment structurée (manquement au principe de *privacy by design* ; en effet, ce principe implique que les responsables du traitement ou sous-traitants disposent d'un système qui permette d'accéder facilement aux données traitées).

Al. 2

Le montant de 300 francs reste inchangé : au sens de l'indice suisse des prix à la consommation, il n'a que peu varié depuis son introduction dans l'ordonnance ; en outre, il ne doit pas avoir d'effet dissuasif pour la personne concernée.

Al. 3

Le responsable du traitement doit informer la personne concernée du montant à payer avant de lui communiquer les renseignements. Si la personne ne confirme pas sa demande dans les dix jours, elle est considérée comme retirée sans occasionner de frais. Le délai prévu à l'art. 18, al. 1, OPDo (ancien art. 22, al. 1, P-OLPD) commence à courir après l'expiration du délai de réflexion de 10 jours.

5.3.2 Section 2 : Droit à la remise et à la transmission des données personnelles

Les articles de la section 2 précisent les différentes exigences applicables au droit à la remise et à la transmission des données qui a été introduit à l'art. 28 nLPD. Compte tenu du fait que l'objectif du Parlement était de créer une réglementation similaire à celle du droit européen, on a tenu compte des règles applicables en matière de portabilité des données inscrites à l'art. 20 RGPD.

Le droit à la remise ou à la transmission des données personnelles confère aux personnes concernées la possibilité, dans certaines conditions, de demander au responsable du traitement de leur fournir les données personnelles qu'elles ont mises à sa disposition, sous une forme permettant leur réutilisation.

Les données personnelles demandées peuvent être réutilisées à différentes fins : pour un usage strictement personnel (p. ex. pour les enregistrer sur un espace de stockage personnel), pour les transmettre à d'autres fournisseurs de services en ligne, ou pour changer de plateforme.

Le droit de demander la transmission des données personnelles confère aux personnes concernées le droit de demander au responsable du traitement de les transmettre directement à un autre responsable (p. ex. pour permettre à un nouveau fournisseur en ligne de compléter ces données, ou lui permettre d'offrir de nouveaux services à la personne, ou encore pour qu'un « historique » personnel puisse être conservé en cas de changement de fournisseur), à condition que cela ne nécessite pas un effort disproportionné.

Il faut bien faire la différence entre le droit à la remise ou à la transmission des données personnelles et le droit d'accès prévu à l'art. 25 nLPD. Le droit d'accès permet à la personne concernée de demander au responsable du traitement des informations, afin de savoir quelles données personnelles la concernant sont traitées. Il lui permet d'exiger la rectification ou l'effacement de ses données personnelles en cas de traitement illicite.

En revanche, le droit à la remise ou à la transmission des données personnelles vise à renforcer le contrôle que peut avoir la personne concernée sur ses données personnelles et leur réutilisation. Il lui permet de disposer elle-même des données personnelles qui ont été utilisées ou transmises, de les réutiliser ou de les transmettre à un autre responsable. Ces personnes pourront par ailleurs plus facilement passer d'un service à un autre, ce qui favorise la concurrence et l'innovation.

Pour les responsables du traitement, ce nouveau droit implique qu'ils devront mettre à disposition, dans un délai raisonnable, les données personnelles demandées sous forme agrégée et faire en sorte qu'elles puissent être réutilisées dans un nouveau système sans que cela ne nécessite un effort disproportionné. Pour ce faire, ils devront utiliser des formats courants et des systèmes de gestion des données standards, afin que les données puissent être réutilisées.

Les responsables devront tenir compte des principes de protection des données et respecter leurs obligations en la matière tant lors de la remise des données personnelles demandées que lors de leur transmission.

Art. 20 Étendue du droit

Al. 1

Cet alinéa précise quelles sont les données personnelles concernées par le droit à la remise ou à la transmission. Ce droit porte sur les données personnelles qui concernent la personne elle-même et celles qui sont traitées de manière automatisée ou avec son consentement en relation avec un contrat (art. 28, al. 1, nLPD).

En premier lieu, les données personnelles conservées sur papier sont exclues de ce droit.

Le droit ne s'applique pas non plus aux responsables du traitement qui traitent des données personnelles dans le cadre de l'accomplissement d'une tâche publique ou dans l'intérêt public. Cela correspond à la réglementation définie à l'art. 20, par. 3, RGPD ainsi qu'à l'objectif, avant tout économique, que vise à satisfaire ce droit à la remise ou à la transmission des données personnelles. Les organes fédéraux qui traitent des données dans le cadre de

l'exécution d'une mission d'intérêt public et en vertu d'une base légale ne sont par conséquent en principe pas concernés. Toutefois, dans la mesure où des organes fédéraux traitent par exemple des données personnelles dans le cadre de la concurrence avec des responsables privés, il est envisageable que ce droit s'applique alors aux données personnelles traitées. Il appartient en tout état de cause au responsable de vérifier si ce droit peut s'appliquer aux données personnelles qu'il traite, et si oui auxquelles, et quelles données sont exclues.

Les données personnelles anonymisées ou celles qui ne concernent pas la personne en question ne font pas l'objet de ce droit. En revanche, les données pseudonymisées qui peuvent clairement être attribuées à la personne concernée sont couvertes par l'art. 20, al. 1, OPDo. En pratique, il est probable que dans de nombreux cas, on ait affaire à des informations contenant des données relatives à plusieurs personnes, comme ce serait le cas avec l'historique du compte d'un client ou celui de conversations téléphoniques ou des messages, qui contiennent des informations sur des tiers. Dans le cadre d'une demande de remise ou de transmission des données personnelles, ces enregistrements devraient aussi être fournis. Les données personnelles de tiers ne doivent toutefois pas être traitées à des fins qui porteraient atteinte à leurs droits ou leur liberté, comme ce serait le cas si les nouveaux responsables utilisaient les données personnelles de tiers transmises à leurs propres fins, notamment pour leur proposer leurs services. Il n'y aurait en revanche pas d'atteinte aux droits ou libertés de tiers si, lors d'un transfert d'informations vers un nouveau compte bancaire à la demande de son titulaire, celui-ci continue à utiliser aux mêmes fins une adresse de contact figurant dans l'historique de son compte, c'est-à-dire uniquement à titre d'adresse de contact et pour son usage personnel.

Par ailleurs, seules les données personnelles que la personne a activement mis à disposition du responsable sont concernées par l'art. 20, al. 1, OPDo. D'après la let. a, il s'agit des données qui ont été *directement* et consciemment fournies : p. ex. données de contact dans un formulaire en ligne ou « likes ». D'après la let. b, il s'agit aussi des données personnelles que la personne a *indirectement* fournies, qui ont été collectées sur la base de son utilisation d'un service ou d'un appareil (délibérément ou non) et observées par le responsable (ce que l'on appelle les données d'utilisation : recherches, journal des activités, ordre de consultation d'un site web).

Le fait que ces types de données soient concernés correspond à la réglementation européenne ainsi qu'au sens et au but de l'art. 28 nLPD selon lequel la personne concernée doit pouvoir demander au responsable qu'il lui remette ou transmette les données personnelles qu'elle lui a communiquées.

Al. 2

L'al. 2 décrit quelles données ne sont pas considérées comme des données personnelles que la personne a communiquées au sens de l'art. 28, al. 1, nLPD et précise de ce fait le champ d'application du droit à la remise ou à la transmission des données personnelles. Ce droit ne porte donc pas sur les données personnelles que le responsable déduit à partir des données personnelles mises à sa disposition par la personne concernée ou observées au sens de l'art. 20, al. 1, let. a et b ainsi que celles générées à partir d'une analyse de ces données. Citons à titre d'exemple l'évaluation de l'état de santé d'un utilisateur, les profils d'utilisateur ou profils à risque, les analyses de risques de crédit, etc. Dans ces cas particuliers, et contrairement aux données mises à disposition par la personne, les prestations et les investissements du responsable se concentrent sur l'analyse et l'évaluation des données fournies, et non pas sur le fait de les collecter et les traiter.

Le fait d'exclure ces données du droit à la remise ou à la transmission de données personnelles correspond à la réglementation européenne en vigueur. Puisque l'objectif de ce droit est de permettre aux personnes concernées de réutiliser leurs données personnelles, il semble justifié de prévoir une exception pour les données qui ont pu être générées par un responsable par le biais d'une analyse ou en mobilisant des ressources (prestations ou investissements propres, algorithmes et méthodes d'analyse internes). Contrairement aux données personnelles mises à disposition par la personne au sens de l'al. 1, les données générées par le responsable doivent être considérées comme plus importantes pour celui-ci s'il souhaite protéger les prestations qu'il a fournies et ses investissements. Elles ne feront par conséquent pas l'objet du droit à la remise ou à la transmission des données personnelles.

Dans le cadre du droit d'accès au sens de l'art. 25 nLPD et des dispositions de l'ordonnance qui s'y rapportent (art. 16 à 19 OPDo), la personne concernée a la possibilité de demander au responsable des informations quant à ces données, la finalité de leur traitement, la durée de conservation, l'existence de décisions individuelles automatisées ainsi que la logique sur laquelle se fondent ces décisions.

Il est important de retenir que l'art. 20, al. 2, OPDo ne constitue pas une limitation du droit à la remise ou à la transmission des données personnelles instauré à l'art. 28 nLPD, mais qu'il vient clarifier la disposition légale en précisant le champ d'application du droit.

En raison du renvoi de l'art. 29, al. 1, nLPD à l'art. 26, al. 1 et 2, nLPD les motifs prévus pour limiter le droit d'accès s'appliquent également au refus, à la restriction, ou au report de la remise ou de la transmission de données personnelles, par exemple pour protéger les intérêts prépondérants du responsable (p. ex. secrets d'affaires ou propriété intellectuelle) ou ceux de tiers. Il ne faut toutefois pas que cela permette de refuser toute transmission d'informations à la personne concernée. Au contraire, il faudra déterminer au cas par cas, en examinant la proportionnalité et en faisant une pesée des intérêts si des données personnelles doivent être remises à la personne concernée ou transmises à un autre responsable, et si oui, lesquelles.

Si le responsable refuse ou restreint la remise ou la transmission de données, ou s'il la reporte, il est obligé d'indiquer à la personne concernée ses motifs, en application de l'art. 29, al. 2, nLPD.

Art. 21 *Exigences techniques de mise en œuvre*

Al. 1

Cette disposition définit ce qui est considéré comme un format électronique couramment utilisé au sens de l'art. 28, al. 1, nLPD. Il s'agit des formats qui permettent, moyennant un effort proportionné, de transmettre les données personnelles en vue de leur réutilisation par la personne concernée ou par un autre responsable du traitement.

Si les données personnelles ne sont pas enregistrées dans un format lisible (en particulier s'il s'agit de formats propriétaires ou peu usités), le responsable devra les convertir dans un format électronique couramment utilisé. Il faut que les personnes concernées puissent directement télécharger leurs données, dans un format informatique standard, à partir de leur compte ou espace personnel. Des formats adaptés au type de données concernées devront être choisis, de préférence des formats ouverts ou permettant l'interopérabilité tels que XML et JSON pour les grandes quantités de données ou CSV, ODT, ODS, etc. De tels formats se prêtent bien à la remise ou à la transmission de données car ils ne posent pas de problèmes notables en matière de compatibilité et peuvent être réutilisés par d'autres responsables

du traitement. Les données enregistrées dans un format difficile à traiter (p. ex. images ou PDF) ou dans un format propriétaire, dont l'utilisation exige l'acquisition d'un logiciel ou l'achat d'une licence ne sont a priori pas adaptées.

De plus, le contenu des informations transmises devra être précisément décrit au moyen de métadonnées appropriées et intelligibles afin qu'elles puissent être réutilisées de manière sensée dans un nouveau système. Les personnes concernées et les responsables du traitement qui reprennent des données qui leur sont transmises doivent pouvoir comprendre à quel type de données ils ont affaire. Les métadonnées doivent être suffisamment complètes pour permettre l'utilisation et la réutilisation des données, sans toutefois divulguer des secrets d'affaires.

Al. 2

Conformément au droit européen, cette disposition précise que le droit de la personne à se voir remettre ses données personnelles ou de les faire transmettre à un autre responsable ne crée pas d'obligation pour le responsable du traitement d'adopter ou de reprendre des systèmes de données techniquement compatibles.

Même si l'introduction de standards de formats de données est en principe possible, le format le plus approprié varie en fonction de la branche et du secteur. Il semble donc suffisant de prévoir l'emploi de formats couramment utilisés, sans spécifier ces formats de manière plus détaillée ou même de façon exhaustive. Du point de vue technique, il est nécessaire que les responsables créent les conditions permettant l'échange de données personnelles. En outre, les données personnelles échangées doivent pouvoir être utilisées par la personne concernée ou le nouveau responsable du traitement. Pour ce faire, les responsables doivent mettre à disposition les données dans un format permettant l'interopérabilité et les décrire à l'aide de métadonnées afin de les rendre compréhensibles pour la personne concernée et le nouveau responsable, et de permettre leur réutilisation.

Al. 3

L'al. 3 précise quand, au sens de l'art. 28, al. 3, nLPD, une transmission nécessite des efforts disproportionnés et quand le responsable n'est pas tenu de transmettre des données personnelles à un autre responsable à la demande de la personne concernée. Une fois de plus, conformément au droit européen, il faut partir du principe qu'un transfert nécessite un effort proportionné lorsque l'opération est techniquement possible et faisable.

Le responsable a l'obligation, à la demande de la personne concernée, de transmettre directement à un autre responsable les données personnelles dans un format interopérable. Même si l'autre responsable ne peut pas prendre en charge ce format, une transmission directe des données peut avoir lieu si les deux systèmes peuvent communiquer de manière sécurisée et que le système destinataire est en mesure de recevoir les données d'un point de vue technique. Il conviendra de vérifier au cas par cas si la transmission est techniquement possible. Il serait également envisageable de mettre à disposition une interface de programmation d'application (API) afin de permettre à l'autre responsable de récupérer les données personnelles de manière automatisée. Si la transmission directe est toutefois impossible en raison de problèmes techniques, le responsable doit en informer la personne concernée (art. 29, al. 2, nLPD).

Le responsable ne doit pas empêcher de manière injustifiée la transmission de données personnelles en dressant des obstacles techniques qui ralentissent ou empêchent l'accès

aux données, leur remise ou leur réutilisation par la personne concernée ou un autre responsable. Ce serait par exemple le cas si l'interopérabilité n'était pas assurée, si l'accès à un format n'était pas possible ou l'accès à une interface de programme n'était pas fourni, ou si la récupération de toutes les données était trop compliquée, si des données étaient délibérément dissimulées, ou si des exigences spécifiques ou injustifiées étaient imposées en matière de normalisation ou d'accréditation dans un secteur spécifique.

Art. 22 Délais, modalités et responsabilité

En ce qui concerne les modalités du droit à la remise ou à la transmission des données, diverses dispositions relatives au droit d'accès s'appliquent par analogie. Il s'agit de la forme dans laquelle la personne concernée peut demander la remise ou la transmission de ses données personnelles (art. 16, al. 1, OPDo, ancien art. 20, al. 1, P-OLPD) et des mesures adéquates qui doivent être prises pour assurer l'identification de la personne concernée et pour protéger ses données de tout accès de tiers non autorisé lors de la communication des renseignements (art. 16, al. 5, OPDo, ancien art. 20, al. 4, P-OLPD).

Les dispositions relatives à la réglementation des responsabilités en matière de demandes d'accès lorsque plusieurs responsables traitent en commun des données personnelles (art. 17, al. 1, OPDo, ancien art. 21, al. 1, P-OLPD), ainsi qu'aux cas où le traitement des données est effectué par un sous-traitant (art. 17, al. 2, OPDo, ancien art. 21, al. 2, P-OLPD) sont applicables par analogie. Il convient de noter que les données personnelles traitées par des sous-traitants sont également soumises au droit à la remise ou à la transmission. Dans ce cas, il incombe au responsable de mettre en place les solutions techniques et organisationnelles permettant de faire valoir ce droit. Le sous-traitant doit aider le responsable à remplir ses obligations en matière de remise et de transmission des données (art. 17, al. 2, OPDo, ancien art. 21, al. 2, P-OLPD).

Enfin, les dispositions relatives aux délais (art. 18 OPDo, ancien art. 22 P-OLPD) et aux exceptions à la gratuité (art. 19 OPDo, ancien art. 23 P-OLPD) sont aussi applicables par analogie.

5.4 Chapitre 4 : Dispositions particulières pour le traitement de données personnelles par des personnes privées

Art. 23 Conseiller à la protection des données

L'art. 10, al. 2, nLPD prévoit, de façon non exhaustive, deux tâches que conseiller à la protection des données d'un responsable du traitement privé devra accomplir : former et conseiller le responsable du traitement dans le domaine de la protection des données (let. a) et concourir à l'application des prescriptions relatives à la protection des données (let. b). Comme ces domaines d'activité découlent de façon suffisamment concrète de la loi, ils ne seront pas définis une nouvelle fois dans l'ordonnance, contrairement à ce qui était prévu dans le P-OLPD.

Let. a et b

Ces dispositions reprennent le contenu de l'art. 12b, al. 2, let. b et c, OLPD.

L'énumération des documents que le conseiller à la protection des données doit pouvoir consulter est harmonisée avec la nouvelle terminologie de la nLPD. Le conseiller ne doit pas avoir un accès illimité, mais seul un accès aux documents dont il a effectivement besoin pour accomplir ses tâches doit lui être octroyé. Par exemple, il ne faut lui donner accès aux

données personnelles que si elles sont nécessaires à l'exécution de ses tâches. Si, par exemple, le conseiller à la protection des données procède à un examen général des prescriptions internes de protection des données ou des processus de traitement des données, il n'a normalement pas besoin de consulter les données personnelles.

L'art. 12b, al. 2, let. a, OLPD n'est en revanche pas repris car la condition qu'il mentionne est dorénavant prévue dans la loi elle-même (art. 10, al. 3, let. a, nLPD).

Let. c

Le responsable doit donner au conseiller à la protection des données le droit d'informer l'organe supérieur de direction ou d'administration dans les cas importants. Il s'agit de la direction du responsable privé, organe qui est également responsable du respect des prescriptions en matière de protection des données. La disposition établit un droit du conseiller à la protection des données à demander l'avis d'une autorité supérieure (*Eskalationsrecht*). Cela est nécessaire pour que le conseiller n'ait pas uniquement à se fonder sur les documents dont il dispose, mais pour qu'il puisse aussi obtenir des informations et documents supplémentaires lors de contrôles internes de l'entreprise au sujet du respect des règles de protection des données. En outre, la disposition garantit que le conseiller puisse, en cas de situations complexes ou d'infractions particulièrement graves, faire un rapport au plus haut organe du responsable ou du sous-traitant, et pouvoir obtenir une décision.

Suppression de l'art. 12a OLPD

Cette disposition est supprimée dans la mesure où son contenu figure désormais dans la loi (art. 10, al. 3, let. b et c, nLPD).

Art. 24 Exception à l'obligation de tenir un registre des activités de traitement

En vertu de l'art. 12 nLPD, les responsables du traitement et les sous-traitants doivent tenir chacun un registre des activités de traitement. Celui-ci doit contenir certaines informations minimales telles que l'identité du responsable du traitement, la finalité du traitement, une description des catégories des personnes concernées et des catégories des données personnelles traitées, les catégories des destinataires, dans la mesure du possible, le délai de conservation des données personnelles ou les critères pour déterminer la durée de conservation ainsi qu'une description générale des mesures visant à garantir la sécurité des données selon l'art. 8 nLPD et, en cas de communication de données personnelles à l'étranger, le nom de l'État en question et les garanties prévues à l'art. 16, al. 2, nLPD (art. 12, al. 2, nLPD).

Pour certaines PME, la tenue d'un tel registre est susceptible d'entraîner une charge administrative disproportionnée par rapport aux risques potentiels des traitements pour la personnalité des personnes concernées. Dans la mesure où, selon l'art. 12, al. 5, nLPD, le Conseil fédéral doit prévoir des exceptions pour les entreprises, y compris les entreprises individuelles, il est logique que l'exécutif soit également autorisé à appliquer ces exceptions aux personnes physiques et aux autres entités juridiques telles que les associations et les fondations. Cela semble approprié, car la tenue du registre, comme pour les PME, pourrait impliquer un effort disproportionné.

L'art. 24 OPDo (ancien art. 26 P-OLPD) concrétise donc l'art. 12, al. 5, nLPD en précisant qui est concerné par cette exception et quels sont les cas dans lesquels les risques d'atteintes à la personnalité au sens de cette disposition sont limités (cf. message, FF 2017 6656). Il prévoit que les entreprises, et autres organismes de droit privé, qui comptent moins de 250

collaborateurs au 1^{er} janvier d'une année, indépendamment du taux d'occupation, ainsi que les personnes physiques soient déliés de leur obligation de tenir un registre des activités de traitement si les traitements ne portent pas sur des données sensibles à grande échelle (let. a) et ne constituent pas un profilage à risque élevé (let. b). L'exigence fixée à l'art. 24, let. a, OPDo correspond à l'art. 22, al. 2, let. a, nLPD. Autrement dit, seules les PME qui effectuent certains traitements à risque élevé sont obligées de tenir un registre des activités de traitement. La mention des traitements constituant un risque élevé est exhaustive. En ce qui concerne la let. a, nous renvoyons aux commentaires relatifs à l'art. 5, al. 1, let. a, OPDo (ancien art. 4, al. 1, let. a, P-OLPD) relatif à l'obligation, pour les personnes privées, d'établir un règlement de traitement.

Les traitements d'importantes quantités de données ou de données concernant un grand nombre de personnes sont notamment considérés comme des traitements portant sur des données sensibles à grande échelle.

Les PME qui traitent des données au sens de l'art. 24, let. a et b doivent uniquement tenir un registre des activités de traitement pour les traitements qui entrent dans cette définition, et non pas pour tous les traitements qu'elles effectuent. Bien entendu, les PME exemptées de cette obligation peuvent volontairement choisir de tenir un registre des activités de traitement. Il s'agit d'un instrument simple et efficace qui permet au responsable traitant régulièrement des données personnelles de garder une vue d'ensemble sur les activités de traitement. Cela peut aussi aider le responsable à respecter d'autres obligations, telles que le devoir d'information.

5.5 Chapitre 5 : Dispositions particulières pour le traitement de données personnelles par des organes fédéraux

5.5.1 Section 1 : Conseiller à la protection des données

Les art. 25 à 28 OPDo (anciens art. 25 à 30 P-OLPD) remplacent l'art. 23 OLPD, qui concerne le conseiller à la protection des données des organes fédéraux.

Art. 25 Désignation

L'art. 25 OPDo met en œuvre l'art. 10, al. 4, nLPD et l'art. 32 de la directive (UE) 2016/680. La règle selon laquelle plusieurs organes fédéraux pourront désigner conjointement un conseiller à la protection des données commun vise surtout à permettre aux organes plus petits ou aux départements avec une structure organisationnelle centralisée d'utiliser des synergies et de faire des économies. À l'inverse, on attend par exemple que les plus grands offices de l'administration fédérale disposent de leur propre conseiller. Naturellement, les organes pourront aussi désigner plusieurs conseillers à la protection des données.

Art. 26 Exigences et tâches

Al. 1

L'art. 26, al. 1, OPDo reprend à la let. a l'exigence posée à l'art. 12a, al. 2, 2^e phrase, OLPD. La let. b dispose que le conseiller à la protection des données de tous les organes fédéraux devra obligatoirement exercer sa fonction de manière indépendante et sans recevoir d'instructions de la part du responsable du traitement (jusqu'à présent, seuls les organes qui souhaitaient être déliés du devoir de déclarer leurs fichiers [voir art. 23, al. 2, OLPD] devaient satisfaire aux exigences des art. 12a et 12b OLPD). Ce principe est repris de l'art. 12b, al. 2, let. a OLPD et il s'agit d'une réglementation similaire à celle relative aux responsables du

traitement privés de l'art. 10, al. 3, let. a, nLPD. Ces règles renforcent et institutionnalisent le rôle du conseiller à la protection des données au sein des organes fédéraux, qui ont en général une hiérarchie stricte, de façon à ce qu'il puisse remplir efficacement son rôle. Le rôle du conseiller à la protection des données est uniquement consultatif et sert de soutien ; le potentiel de conflit avec les services responsables ou supérieurs doit donc être considéré comme limité. Il faut néanmoins garantir que le conseiller à la protection des données puisse formuler ses recommandations librement (même si elles peuvent être déplaisantes de par leur nature) sans avoir à craindre de préjudices. L'indépendance implique également que le conseiller puisse s'adresser à l'organe supérieur de l'administration dans les cas importants, comme le prévoit explicitement l'art. 23, let. c, OPDo pour les responsables privés. L'indépendance doit surtout être garantie par le biais de mesures organisationnelles : il faut éviter que la fonction de conseiller à la protection des données ait un impact négatif sur l'évaluation du collaborateur concerné.

Al. 2

La terminologie utilisée pour décrire les tâches du conseiller à la protection des données d'un organe fédéral prescrites à l'al. 2 est modifiée pour correspondre à la disposition relative aux conseillers des responsables privés (art. 10, al. 3, nLPD). L'al. 2, let. a, dispose que le conseiller à la protection des données participe à l'application des règles de protection des données, comme déjà mentionné à l'art. 10, al. 2, let. b, nLPD. Cela implique notamment que, selon le ch. 1, il contrôle le traitement des données personnelles et propose des mesures correctives lorsqu'une violation des dispositions relatives à la protection des données est constatée et que, selon le ch. 2, il conseille le responsable du traitement lors de l'établissement de l'analyse d'impact relative à la protection des données et en vérifie l'exécution. La participation du conseiller à la protection des données peut contribuer à décharger le PFPDT. L'exigence fixée au ch. 2 correspond à l'art. 7, let. c de la directive (UE) 2016/680.

Le conseiller à la protection des données a une fonction de conseil et de soutien mais n'est pas un organe de surveillance. En ce qui concerne la vérification des traitements et la recommandation de mesures correctives, il convient de noter qu'il ne s'agit pas d'instaurer une obligation de vérification ou des contrôles systématiques de tous les traitements de données. Il suffit que le conseiller agisse, par exemple, lorsque les organes responsables lui posent des questions relatives à l'évaluation du traitement des données, ou s'il reçoit des informations concernant une violation des prescriptions de protection des données. Bien entendu, le conseiller est libre de procéder à des contrôles proactifs. Le conseiller à la protection des données sert, selon l'al. 2, let. b, de point de contact pour les personnes concernées, par exemple lorsqu'elles adressent une demande d'accès au sens de l'art. 25 nLPD.

Art. 27 Devoirs de l'organe fédéral

L'art. 27, al. 1, let. a, OPDo (ancien art. 29, al. 1, P-OLPD) est identique aux dispositions valant pour les responsables privés, soit l'art. 22, let. b, OPDo (ancien art. 25, al. 2, let. b, P-OLPD). Nous renvoyons aux commentaires à ce sujet. S'il existe des bases légales spéciales qui empêchent le conseiller à la protection des données d'accéder à certaines informations, en particulier les données personnelles, celles-ci priment, conformément au principe *lex specialis derogat generali*. Si nécessaire, les données personnelles doivent être caviardées si le conseiller à la protection des données a besoin d'accéder à des informations concernant des données personnelles pour exercer ses tâches. Selon l'art. 27, al. 1, let. b, OPDo, l'organe fédéral doit veiller à ce que le conseiller à la protection des données soit informé de toute violation de la sécurité des données. Ce devoir peut par exemple être rempli lorsque

l'organe fédéral oblige ses collaborateurs, par le biais de directives, à informer le conseiller des cas de violation de la sécurité des données. Le devoir concerne toutes les violations, et pas uniquement celles qui doivent être annoncées au PFPDT en vertu de l'art. 24 nLPD. Le conseiller à la protection des données conseille le responsable pour savoir si la violation doit être annoncée au PFPDT conformément à l'art. 24 nLPD. Il revient toutefois au responsable de se charger de l'annonce : c'est lui qui décide si des violations doivent être annoncées au PFPDT, et si oui, lesquelles.

L'al. 2 est nouveau ; il prévoit une règle similaire à celle fixée à l'art. 10, al. 3, let. d, nLPD pour les responsables privés. Il facilitera l'exercice des droits des personnes concernées dans la mesure où elles pourront immédiatement trouver un interlocuteur spécialisé à contacter. Il n'est pas nécessaire de rendre public le nom du conseiller : il suffira par exemple d'indiquer l'adresse électronique de l'organe compétent. Les coordonnées du conseiller à la protection des données devront aussi être communiquées au PFPDT.

Art. 28 Interlocuteur du PFPDT

L'art. 28 OPDo (ancien art. 30 P-OLPD) reprend sur le fond, mais de façon plus précise, l'art. 23, al. 3, OLPD. La formulation est adaptée parce qu'elle pouvait être mal interprétée et comprise comme une interdiction de contact direct. Les organes fédéraux devraient également être libres de communiquer avec le PFPDT par le biais d'autres entités et pas uniquement au travers du conseiller à la protection des données. Il ne fait pas office d'agent de liaison pour le PFPDT, mais plutôt d'interlocuteur, car il dispose de l'expertise et des connaissances internes nécessaires pour répondre aux questions relatives au traitement des données personnelles effectué par l'organe fédéral auquel il appartient.

5.5.2 Section 2 : Devoir d'informer

Art. 29 Devoir d'informer lors de la communication des données personnelles

Cette disposition correspond aux art. 12 et 26 OLPD et concerne la fiabilité des données personnelles communiquées. Outre l'« actualité » et la « fiabilité » des données, leur « exhaustivité » est mentionnée à l'art. 29 OPDo (ancien art. 15 P-OLPD). Pour assurer la qualité des données, celles-ci doivent être actuelles, fiables et complètes (c'est-à-dire ni partielles, ni lacunaires). Cette disposition est ainsi alignée avec l'art. 7, par. 2 de la directive (UE) 2016/680. Elle vient compléter l'art. 6, al. 5, nLPD.

Art. 30 Devoir d'informer lors de la collecte systématique des données personnelles

Cette disposition correspond à l'art. 24 OLPD : si la personne concernée n'est pas tenue de fournir des renseignements, l'organe fédéral compétent doit l'informer du caractère facultatif de sa réponse. Conformément à la disposition de l'art. 24 OLPD, cette obligation n'est valable que lorsqu'il s'agit d'une collecte systématique de données personnelles. Elle concerne surtout les domaines de la statistique et de la recherche.

5.5.3 Section 3 : Annonce au PFPDT des projets pour le traitement automatisé des données personnelles

Art. 31

L'art. 31, al. 1, OPDo dispose que l'organe fédéral compétent doit informer le PFPDT des activités de traitement automatisé prévues dès l'approbation du projet ou dès la décision de développement. Contrairement à l'annonce subsidiaire au PFPDT selon l'art. 20, al. 2,

OLPD, qui a pour objectif un examen matériel des projets, l'annonce au PFPDT sert à établir un simple aperçu des projets dans le cadre desquels des activités de traitement automatisé sont prévues. Cela permet au PFPDT d'optimiser la planification de ses ressources entre les activités de conseil et l'accompagnement de projets législatifs. En second lieu, cette annonce sert aussi évidemment à la protection de la personnalité.

Puisqu'au moment de cette annonce, les projets sont encore à un stade peu avancé, le contenu de cette annonce, au sens de l'al. 2, se limite à une partie des indications exigées à l'art. 12, al. 2, nLPD, soit à celles figurant aux lettres a à d. Tout comme la déclaration des registres des activités de traitement déjà existantes selon l'art. 12 nLPD, le PFPDT enregistre les activités planifiées dans le registre des activités de traitement au sens de l'art. 56 nLPD. Les informations relatives à l'annonce des activités de traitement planifiées ne sont toutefois pas rendues publiques (voir art. 42, al. 2 OPDo). D'après l'al. 4, l'organe fédéral compétent actualise l'annonce lorsque le projet est achevé avec succès, c'est-à-dire lors du passage à la phase de production (respectivement, il transforme cette annonce en une déclaration au sens de l'art. 12, al. 4, nLPD) ou lorsque le projet est abandonné (ce qui implique la suppression de l'inscription). Ainsi l'annonce n'est « visible » pour le PFPDT qu'au moment de l'approbation du projet ou de la décision de le développer.

5.5.4 Section 4 : Essais pilotes

Art. 32 Caractère indispensable de l'essai pilote

En vertu de l'art. 35, al. 1, nLPD, le Conseil fédéral peut autoriser, avant l'entrée en vigueur d'une loi au sens formel, le traitement automatisé de données sensibles ou d'autres traitements au sens de l'art. 34, al. 2, let. b et c, nLPD si certaines conditions cumulatives sont réunies. L'une de ces conditions est que la mise en œuvre du traitement rende indispensable une phase d'essai avant l'entrée en vigueur de la loi au sens formel, en particulier pour des raisons techniques. Dans le souci de diminuer la densité normative de l'art. 35 nLPD, le Conseil fédéral a en effet décidé de déplacer ces précisions de l'art. 17a, al. 2, LPD pour les inscrire dans l'ordonnance.

L'art. 32 OPDo définit les cas dans lesquels une phase d'essai pilote peut être considérée comme indispensable. Il reprend, moyennant quelques modifications rédactionnelles, l'art. 17a, al. 2, LPD. Le sens du terme d'« innovations techniques » n'a pas changé : il s'agit tant du recours à de nouvelles technologies que le recours à des technologies connues, mais dans un nouvel environnement, ou utilisées dans de nouvelles solutions. L'application SwissCovid³⁵ en est un exemple : bien qu'elle se fonde sur des technologies connues, telles que le Bluetooth, elle n'a pas encore d'équivalent. Seule la let. c a subi des modifications : selon la nouvelle formulation, les données ne devront plus être accessibles en ligne uniquement aux autorités cantonales. L'ancienne formulation était plus restrictive, pour des raisons historiques. Toutefois, en l'espèce, ce n'est pas la personne qui accédera aux données en ligne qui doit être le critère décisif, mais c'est l'aspect technique qui sera déterminant pour supposer le caractère indispensable de la phase d'essai (voir art. 35, al. 1, let. c, nLPD).

Au moins l'une des conditions des let. a à c doit être remplie : cela signifie qu'il n'est pas possible de lancer un essai pilote uniquement pour des raisons de temps.

³⁵ Voir art. 60a de la loi fédérale du 28 septembre 2012 sur les épidémies (RS 818.101) et l'ordonnance du 24 juin 2020 sur le système de traçage de proximité pour le coronavirus SARS-CoV2 (RS 818.101.25).

Art. 33 Procédure d'autorisation de l'essai pilote

Cette disposition reprend 27 OLPD moyennant des modifications d'ordre rédactionnel. Les renvois à la nLPD ont été adaptés. Un nouvel al. 6 est ajouté : il précise, comme c'est le cas actuellement à l'art. 17a, al. 3, LPD, que le traitement automatisé doit être réglé par voie d'ordonnance. Cela permettra d'assurer la transparence des essais pilotes.

Art. 34 Rapport d'évaluation

Cette disposition reprend l'art. 27a OLPD.

L'art. 34 OPDo indique que l'organe fédéral soumet pour avis au PFPDT le projet de rapport d'évaluation. S'il l'estime nécessaire, l'organe fédéral responsable adapte le rapport d'évaluation.

5.5.5 Section 5 : Traitements des données à des fins ne se rapportant pas à des personnes

Art. 35

Afin d'assurer que les mesures dérogatoires prévues à l'art. 39, al. 2, nLPD ne soient pas appliquées au-delà de ce que prévoit la loi, il est précisé dans l'ordonnance que lorsqu'un traitement à des fins ne se rapportant pas à des personnes (par exemple un traitement à des fins de recherche, de planification ou de statistique) sert dans le même temps une autre finalité, lesdites dérogations ne sont applicables qu'au seul traitement effectué aux fins visées par l'art. 39 nLPD.

5.6 Chapitre 6 : Préposé fédéral à la protection des données et à la transparence

Art. 36 Siège et secrétariat permanent

La disposition correspond à l'art. 30 OLPD.

En comparaison avec l'article 30 OLPD, l'art. 36, al. 1, OPDo (ancien art. 37, al. 1, P-OLPD) reste inchangé du point de vue matériel. Le secrétariat n'est plus mentionné, car le remplacement du terme « préposé » par « PFPDT » indique que l'on évoque ici l'autorité dans son ensemble, ce qui inclut aussi son secrétariat.

L'art. 36, al. 2, OPDo (ancien art. 37, al. 1, P-OLPD) règle les rapports de travail du secrétariat permanent du PFPDT. Sur le fond, cette disposition équivaut à l'actuel art. 30, al. 2, OLPD mais elle a été adaptée du point de vue terminologique et complétée. Le préposé et le secrétariat permanent du PFPDT constituent, en vertu de la LPD révisée, une entité administrative décentralisée sans personnalité juridique rattachée administrativement à la Chancellerie fédérale (art. 43, al. 4, 2^e phrase, nLPD, art. 2, al. 1, let. e LPers³⁶, art. 2, al. 3 de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration [LOGA]³⁷ et art. 8, al. 1, let. b en relation avec l'annexe 1, let. a, ch. 2.1.1 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration [OLOGA]³⁸). Comme c'est déjà le cas, l'art. 43, al. 5, 2^e phrase, nLPD prévoit que le préposé engage son personnel et qu'il dispose dans ce contexte de certaines compétences. Par exemple, les contrats de travail du personnel du PFPDT sont signés par le préposé. Celui-ci n'est cependant toujours pas un

³⁶ RS 172.220.1

³⁷ RS 172.010

³⁸ RS 172.010.1

employeur au regard du droit du personnel et de la prévoyance au sens de la LPers. D'après l'art. 3, al. 1, let. a, LPers, l'employeur est le Conseil fédéral. Selon l'art. 36, al. 2, 1^{ère} phrase, OPDo, la législation sur le personnel de la Confédération continue de s'appliquer aux rapports de travail du secrétariat permanent du PFPDT. Ainsi l'ordonnance du 3 juillet 2001 sur le personnel de la Confédération (OPers)³⁹, l'ordonnance du 6 décembre 2001 du DFF concernant l'ordonnance sur le personnel de la Confédération (O-OPers)⁴⁰ et l'ordonnance du 22 novembre 2017 concernant la protection des données personnelles du personnel de la Confédération (OPDC)⁴¹ restent applicables. L'art. 30, al. 2, OLPD est uniquement adapté du point de vue terminologique (« secrétariat du préposé » est remplacé par « personnel du secrétariat permanent du PFPDT » et « la loi du 24 mars 2000 sur le personnel de la Confédération et ses dispositions d'exécution » est remplacée par « la législation fédérale sur le personnel »). En outre, l'art. 36, al. 2, 2^e phrase, OPDo précise que le personnel du secrétariat permanent du PFPDT est assuré auprès de la Caisse de prévoyance de la Confédération. Cet ajout n'entraîne aucune modification matérielle mais reprend, expressément, la disposition existante concernant le secrétariat permanent du PFPDT (voir art. 32a, al. 1 et 32d, al. 1, LPers). Le personnel reste donc assuré conformément aux dispositions du règlement de prévoyance du 15 juin 2007 pour les personnes employées et les bénéficiaires de rentes de la Caisse de prévoyance de la Confédération (RPEC)⁴².

Le statu quo est pour le moment maintenu en ce qui concerne les rapports de travail du secrétariat permanent du PFPDT. Cela se justifie notamment parce que le rattachement administratif à la Chancellerie fédérale permet au PFPDT de consacrer ses ressources aux tâches opérationnelles. La collaboration entre la Chancellerie et le PFPDT est organisée de façon à garantir son indépendance. Néanmoins, la question se pose de savoir si le préposé devrait se voir octroyer des compétences d'employeur en matière de droit du personnel et de la prévoyance vis-à-vis des employés du secrétariat permanent. Il faudra traiter cette question au niveau de la loi à la prochaine occasion qui se présente. La vérification et l'adaptation coordonnée des lois spéciales sur le traitement des données concernant des personnes morales, qui devrait avoir lieu dans les cinq ans suivant l'entrée en vigueur de la nLPD (voir art. 71 nLPD), pourrait être une occasion de régler cette question.

Les dispositions d'exécution concernant les rapports de travail du préposé ne doivent pas être édictées par le Conseil fédéral, mais par l'Assemblée fédérale car ces rapports de travail seront établis par son élection (art. 43, al. 1, nLPD). Dans le cadre de l'initiative parlementaire 21.443, la Commission des institutions politiques du Conseil national a adopté le 27 janvier 2022 un projet d'ordonnance de l'Assemblée fédérale qui contient les dispositions d'exécution relatives aux rapports de travail du préposé. En outre, des modifications ponctuelles de la nLPD sont prévues dans ce contexte. Le Parlement a adopté les projets en vote final le 17 juin 2022.

L'art. 30, al. 3, OLPD n'est pas conservé parce que le PFPDT possède désormais son propre budget, qui est réglé de façon exhaustive à l'art. 45 nLPD et à l'art. 142, al. 2 et 3 de la loi du 13 décembre 2002 sur le Parlement (nLParl)⁴³.

³⁹ RS 172.220.111.3

⁴⁰ RS 172.220.111.31

⁴¹ RS 172.220.111.4

⁴² RS 172.220.141.1

⁴³ RS 171.10 [FF 2020 7397, 7437]

Art. 37 Voie de communication

L'art. 37 OPDo est largement repris de l'art. 31, al. 1 et 1^{bis} OLPD. L'art. 31, al. 2 n'est pas conservé dans l'OPDo car le PFPDT peut communiquer directement avec d'autres unités administratives dans la mesure où il est indépendant et peut agir sans recevoir d'instructions. La suppression n'entraîne aucune modification matérielle. Par rapport à l'art. 31 OLPD, l'al. 1 est modifié. La nouvelle formulation vise à préciser que le PFPDT peut également prendre contact avec le Conseil fédéral pour des questions qui ne figurent pas à l'ordre du jour d'une réunion du Conseil fédéral, en communiquant des prises de position, par exemple. Mis à part cet aspect, le contenu de l'al. 1 est inchangé, puisque le Chancelier fédéral doit transmettre toutes les communications au Conseil fédéral et n'a pas de marge de manœuvre sur ce point. Cela concerne également la procédure de co-rapports. Seule la formulation du deuxième alinéa a subi de légères modifications : sur le fond, il correspond à l'art. 31, al. 1^{bis}, OLPD.

Art. 38 Communication des décisions, des directives et des projets

Hormis les modifications terminologiques et systématiques, cette disposition correspond à l'art. 32, al. 1, OLPD.

Selon l'al. 2, il faut associer le PFPDT aux projets législatifs le plus tôt possible : celui-ci devrait au plus tard être entendu au moment de la consultation des offices.

Art. 39 Traitement des données

Dans le droit en vigueur, l'art. 32, al. 2, OLPD détermine à quelles fins le PFPDT peut gérer un système d'information et de documentation. Le nouvel art. 57h LOGA élaboré dans le cadre de la révision totale de la LPD dispose, de façon générale, que les unités de l'administration fédérale gèrent des systèmes électroniques pour la gestion de leurs documents. Il n'est plus nécessaire que l'OPDo fasse référence à l'utilisation du système de gestion des affaires.

En revanche, les finalités du traitement de données par le PFPDT sont réglées plus en détail (al. 1). Il peut traiter des données personnelles, y compris des données sensibles, notamment aux fins suivantes : exercer ses activités de surveillance (let. a), exercer ses activités de conseil (let. b), collaborer avec les autorités cantonales, fédérales et étrangères (let. c), exécuter des tâches dans le cadre des dispositions pénales au sens de la LPD (let. d), mettre en œuvre des procédures de conciliation et émettre des recommandations au sens de la loi du 17 décembre 2004 sur la transparence (LTrans)⁴⁴ (let. e), mettre en œuvre des évaluations au sens de la LTrans (let. f), mettre en œuvre des procédures de demande d'accès au sens de la LTrans (let. g), informer la surveillance parlementaire (let. h), informer le public (let. i) et exercer des activités de formation (let. j).

Art. 40 Autocontrôle

L'art. 48 nLPD prévoit que le PFPDT doit prendre des mesures appropriées pour s'assurer que les règles de protection des données sont bien respectées et appliquées au sein de son institution. Le message relatif à la nLPD précise que le Conseil fédéral a pour tâche de concrétiser, dans l'ordonnance, les mesures que le PFPDT doit prendre (FF 2017 6565, 6705).

⁴⁴ SR 152.3

Il est attendu du PFPDT, à l'art. 40 OPDo, qu'il établisse un règlement de traitement pour tous les traitements automatisés et pas uniquement dans le cas des traitements particuliers, listés à l'art. 6, al. 1, OPDo, tels que le traitement de données sensibles ou le profilage.

Même si cela n'est pas expressément mentionné (contrairement à l'art. 41, al. 2, P-OLPD), le PFPDT, tout comme les autres organes fédéraux tenus d'établir un règlement de traitement (voir art. 6 OPDo), devra prévoir des processus internes pour garantir que le traitement de données soit effectué conformément au règlement de traitement et vérifier que celui-ci soit respecté.

Art. 41 Collaboration avec le NCSC

Afin que le PFPDT puisse recourir aux spécialistes du Centre national pour la cybersécurité (NCSC) lorsqu'il doit analyser une violation de la sécurité des données qui lui a été annoncée par un responsable du traitement, conformément à l'art. 24 nLPD et à l'art. 15 OPDo (ancien art. 19 P-OLPD), l'art. 41, al. 1, OPDo (ancien art. 42 P-OLPD) prévoit qu'il peut transmettre les informations relatives à ce type d'annonce au NCSC. Le PFPDT peut transmettre toutes les informations énumérées à l'art. 15, al. 1, OPDo mais en se limitant aux données nécessaires pour que le NCSC puisse analyser l'incident. Ainsi, la communication du PFPDT au NCSC peut contenir des données personnelles. Il faut au préalable qu'il ait reçu l'accord du responsable du traitement qui est, quant à lui, obligé d'annoncer ces incidents au PFPDT. En outre, la transmission de ces informations ne doit pas permettre de contourner l'art. 24, al. 6, nLPD d'après lequel l'annonce ne peut être utilisée dans le cadre d'une procédure pénale qu'avec le consentement de la personne tenue d'annoncer. L'art. 41, al. 1, OPDo ne permet pas au PFPDT de systématiquement transmettre les annonces au NCSC. Il ne pourra faire usage de cette possibilité que dans des cas particuliers, lorsque les connaissances techniques du NCSC sont nécessaires pour analyser un incident. Cette disposition devra être transférée dans la loi à la prochaine occasion. C'est pourquoi un nouvel art. 24, al. 5^{bis}, nLPD est prévu à l'annexe de l'avant-projet de modification de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information (LSI)⁴⁵ que le Conseil fédéral a envoyé en consultation le 12 janvier 2022⁴⁶. Celui-ci réglera la transmission par le PFPDT au NCSC de données personnelles sensibles relative à des poursuites ou à des sanctions pénales ou administratives visant le responsable tenu à l'obligation de signalement. Si le nouvel art. 24, al. 5^{bis}, nLPD entre en vigueur, l'art. 41, al. 1, OPDo pourra être abrogé.

L'art. 41, al. 2, OPDo établit que le PFPDT et le NCSC doivent se coordonner lorsque leurs domaines d'activité se recoupent. Cette norme équivaut à l'art. 20, al. 3, 2^e phrase, OLPD. La disposition oblige le PFPDT à inviter le NCSC à se prononcer avant d'ordonner à l'organe fédéral de prendre les mesures visées à l'art. 8 nLPD. La base légale pour une telle obligation est l'art. 51, al. 3, let. b, nLPD. Il s'agit d'éviter que le PFPDT et le NCSC n'imposent aux organes fédéraux des exigences différentes dans le même domaine. L'indépendance du PFPDT restera garantie : bien qu'il doive demander l'avis du NCSC, il ne devra pas nécessairement en tenir compte.

Art. 42 Registre des activités de traitement des organes fédéraux

En raison de l'art. 12, al. 4, nLPD, les organes fédéraux et leurs sous-traitants doivent déclarer leurs registres d'activités de traitement au PFPDT. Il est ensuite exigé de celui-ci, au sens

⁴⁵ RS 126 [FF 2020 9665]

⁴⁶ Les documents soumis à la consultation peuvent être consultés sur : [Ouverture de la consultation relative à l'introduction d'une obligation de signaler les cyberattaques \(admin.ch\)](https://www.admin.ch/gov/fr/accueil/documentation/communiqués.msg-id-86768.html) < <https://www.admin.ch/gov/fr/accueil/documentation/communiqués.msg-id-86768.html> >.

de l'art. 56 nLPD, qu'il tienne un registre des activités de traitement des organes fédéraux et qu'il le publie.

L'art. 42, al. 1, OPDo précise ce que le registre du PFPDT doit contenir, à savoir les informations obligatoirement fournies par les organes fédéraux et leurs sous-traitants sur la base de l'art. 12, al. 2, nLPD. Le registre contient aussi des informations relatives aux activités de traitement automatisées prévues par les organes fédéraux selon l'art. 31, al. 2, OPDo.

Le deuxième alinéa précise que le registre du PFPDT doit être publié en ligne. Les inscriptions au registre concernant les activités de traitement automatisées prévues par les organes fédéraux selon l'art. 31 OPDo ne sont en revanche pas publiées puisqu'elles ne sont pas encore considérées comme définitives au moment où elles sont annoncées et peuvent encore faire l'objet de modifications.

Art. 43 Codes de conduite

En vertu de l'art. 22, al. 5, nLPD, le responsable du traitement privé peut renoncer à établir une analyse d'impact lorsqu'il est certifié conformément à l'art. 13 nLPD ou qu'il se conforme à un code de conduite au sens de l'art. 11 nLPD remplissant certaines conditions. Lorsqu'un code de conduite est soumis au PFPDT, celui-ci indique dans sa prise de position s'il estime que les conditions pour pouvoir renoncer à établir une analyse d'impact relative à la protection des données personnelles sont remplies. Cette disposition permet de préciser que le responsable du traitement qui veut renoncer à une analyse de traitement doit soumettre son code de conduite au PFPDT et celui-ci doit pouvoir l'évaluer. Il ne s'agit pas d'une décision d'approbation, mais dans le cas où un responsable du traitement se prévaudrait de l'exception de l'art. 22, al. 5, let. a à c et ce contrairement à la position du PFPDT, celui-ci peut alors lui ordonner d'établir une analyse d'impact relative à la protection des données sur la base de l'art. 51, al. 3, let. d, nLPD.

Art. 44 Émolument

En vertu de l'art. 59, al. 1, nLPD, le préposé est tenu de percevoir un émolument pour certaines prestations fournies aux personnes privées, à savoir la prise de position sur les codes de conduite (let. a), l'approbation des clauses type de protection des données et des règles d'entreprise contraignantes (let. b), l'examen de l'analyse d'impact relative à la protection des données (let. c), les mesures provisionnelles et celles prononcées en vertu de l'art. 51 nLPD (let. d), ainsi que les conseils en matière de protection des données (let. e).

L'art. 59, al. 2, nLPD charge le Conseil fédéral de fixer le montant des émoluments.

L'art. 44, al. 1, OPDo (ancien art. 44 al. 1, P-OLPD) pose le principe selon lequel l'émolument se calcule en fonction du temps consacré. Le tarif horaire est fixé à l'al. 2. Celui-ci varie entre 150 et 250 francs selon la fonction exercée par la personne concernée. Le montant est basé sur le tarif horaire du personnel de la fonction requise pour pouvoir fournir la prestation. Le PFPDT calcule donc les émoluments sur la base des heures de travail effectuées. Toute personne ayant contribué à la réalisation de la prestation doit être incluse dans ce calcul. Selon l'al. 3, le PFPDT a la possibilité de percevoir des suppléments pouvant atteindre 50% de l'émolument prévu à l'al. 2 pour les prestations d'une ampleur extraordinaire, présentant des difficultés particulières ou ayant un caractère urgent. Cette règle précise le principe général fixé à l'art. 5, al. 3, de l'ordonnance générale sur les émoluments du 8 septembre 2004

(OGEmol)⁴⁷. Si la prestation du PFPDT peut être réutilisée à des fins commerciales par la personne assujettie à l'émolument, le PFPDT peut, conformément à l'al. 4, percevoir des suppléments pouvant atteindre 100% de l'émolument prévu à l'al. 2. Par exemple, si le PFPDT évalue un outil qui peut être revendu par le requérant en tant qu'application conforme aux exigences de la protection des données, le PFPDT doit avoir la possibilité de majorer l'émolument de sorte qu'il corresponde approximativement au salaire horaire d'un avocat spécialisé. L'élément déterminant est de savoir si la prestation pourrait être réutilisée à des fins commerciales, indépendamment du fait que cela se produise ou non. La réglementation prévue à l'al. 4 concerne en particulier le cas de conseils en matière de protection des données au sens de l'art. 59, al. 1, let. e, nLPD. Néanmoins, il est aussi envisageable que le PFPDT évalue des clauses standards de protection des données ou des codes de conduite qui peuvent être réutilisés à des fins commerciales, par exemple parce qu'ils peuvent servir de modèle pour d'autres clauses standard ou codes de conduite. Par ailleurs, l'al. 5 dispose que l'OGEmol s'applique pour le surplus. Cette ordonnance règle notamment les principes applicables à la perception d'émoluments, les exceptions concernant cette obligation, ainsi que la procédure d'encaissement.

5.7 Chapitre 7 : Dispositions finales

Art. 45 Abrogation et modification d'autres actes

Les dispositions relatives à l'abrogation et la modification d'autres actes sont présentées dans une annexe parce qu'elles couvrent plus d'une page. Elles sont commentées ci-dessous au ch. 7.

Art. 46 Dispositions transitoires

L'art. 4, al. 2, OPDo oblige les organes fédéraux responsables et leurs sous-traitants à journaliser les traitements automatisés de données personnelles. Pour les traitements de données qui tombent dans le champ d'application de la directive (UE) 2016/680, l'obligation de journaliser s'applique depuis l'entrée en vigueur de la loi sur la protection des données Schengen, conformément à l'art. 25 de la directive. Plusieurs organes fédéraux ont fait état d'une surcharge de travail liée à la mise en œuvre de l'art. 4, al. 2, OPDo. Pour tenir compte de ce travail supplémentaire, l'art. 46, al. 1, prévoit un délai transitoire de trois ans à compter de l'entrée en vigueur de l'ordonnance ou au plus tard jusqu'à la fin du cycle de vie du système. Pendant cette période, les traitements sont régis par l'art. 4, al. 1, OPDo.

L'art. 8, al. 5, OPDo introduit l'obligation de publier les évaluations. L'al. 2 de l'art. 46 dispose que les évaluations effectuées avant l'entrée en vigueur ne seront pas rendues publiques.

En vertu de l'art. 31 OPDo, les organes fédéraux devront annoncer au PFPDT les activités prévues de traitement automatisé au moment de l'approbation du projet ou de la décision de le développer. L'al. 3 dispose que l'art. 31 OPDo ne s'appliquera pas aux activités prévues de traitement automatisé pour lesquelles l'approbation du projet ou la décision de le développer aura déjà été prise au moment de l'entrée en vigueur de l'ordonnance.

⁴⁷ RS 172.041.1

6 Commentaire relatif à l'annexe 1 (États, territoires, secteurs déterminés dans un État et organismes internationaux dans lesquels un niveau de protection adéquat est garanti)

En raison de l'art. 16, al. 1, nLPD, le Conseil fédéral est compétent et a pour tâche de décider quel État (ou territoire ou secteur déterminé de l'État), ainsi que quel organisme international garantit un niveau de protection adéquat pour la communication des données personnelles à l'étranger.

Une liste de ces États est publiée en annexe de l'ordonnance. L'objectif de cette liste est d'atteindre un espace uniforme en matière de protection des données. La liste sera revue périodiquement afin de prendre en compte d'une part la pratique d'autres États et d'autre part les développements au niveau international, en particulier les ratifications de la Convention 108+. La liste n'est donc pas définitive et pourrait encore être modifiée avant l'entrée en vigueur de l'ordonnance.

L'évaluation du niveau de protection adéquat n'inclut les transferts de données à des fins répressives que lorsque cela est précisé dans l'annexe. Ainsi, la mention d'un astérisque (*) signifie que l'évaluation du niveau de protection adéquat inclut les transferts de données conformément à la directive (UE) 2016/680⁴⁸ tandis que la mention d'un double astérisque (**) indique que de tels transferts sont inclus en vertu d'une décision d'exécution de la Commission européenne constatant le caractère adéquat du niveau de protection des données conformément à la directive (UE) 2016/680 (actuellement c'est le cas pour le Royaume-Uni). Enfin, la mention d'un triple astérisque (***) signifie que l'évaluation du niveau de protection adéquat n'inclut pas les transferts de données dans le cadre de la coopération prévue par la directive (UE) 2016/680.

7 Commentaire relatif à l'annexe 2 (abrogation et modification d'autres actes)

7.1 Abrogation de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données

Comme l'OPDo est une révision totale de l'OLPD, celle-ci doit être abrogée.

7.2 Aperçu des modifications d'ordonnances sectorielles

Le droit de la protection des données est un sujet transversal : de ce fait, les modifications effectuées dans la nLPD et l'OPDo doivent être répercutées dans les dispositions des ordonnances sectorielles relatives à la protection des données.

Les modifications apportées sont avant tout d'ordre terminologique. Les principaux changements sont les suivants :

- Le terme de « profils de la personnalité » est supprimé et remplacé par celui de « profilage » dans la nLPD⁴⁹. Lorsque ce terme est simplement supprimé dans une loi sectorielle, il doit aussi être supprimé dans les ordonnances qui s'y rapportent ; lorsqu'il est remplacé par la nouvelle formulation, celle-ci doit aussi remplacer l'ancien terme dans les ordonnances.

⁴⁸ 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.

⁴⁹ Voir les explications du Message du 15 septembre 2017 concernant la LPD (FF 2017 6565, 6641, 6724).

- La notion de « fichier » est elle aussi supprimée dans la nLPD⁵⁰. Elle est le plus souvent remplacée par « banque de données », « traitement de données », « ensemble de données » ou « collecte de données » dans les ordonnances sectorielles. Si le terme n'est pas utilisé dans un contexte lié aux dispositions en matière de protection des données, il n'est pas nécessaire de le modifier. Le terme de « maître du fichier » est remplacé par celui de « responsable du traitement », conformément à l'art. 5, let. j, nLPD.
- Au niveau des lois, une distinction est faite entre la fonction de préposé fédéral à la protection des données et à la transparence et l'institution dans son ensemble. On se réfère à l'institution au moyen de l'abréviation « PFPDT », et le terme de « préposé » est réservé au chef de l'institution. Les adaptations nécessaires ont été reportées dans les ordonnances sectorielles.
- En allemand, l'expression « Daten über administrative und strafrechtliche Verfolgungen und Sanktionen » est systématiquement remplacée par « Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen », comme à l'art. 5, let. c, ch. 5, nLPD.

Les renvois à la nLPD et à l'OPDo doivent aussi être adaptés dans les ordonnances sectorielles. Il faut aussi procéder à une adaptation des renvois lorsque la LPD est mentionnée dans les préambules de certaines ordonnances.

Les données des personnes morales n'entrent plus dans le champ d'application de la loi selon la nLPD⁵¹. Le terme de « données personnelles » concerne uniquement les données des personnes physiques. Par conséquent, les bases légales qui donnent aux organes fédéraux le pouvoir de traiter et communiquer les données personnelles ne seront plus applicables aux données des personnes morales. En raison du principe de la légalité, il est encore nécessaire qu'il existe une base légale pour le traitement et la communication de données des personnes morales par la Confédération. Celle-ci sera en partie fixée dans la LOGA. Par ailleurs, il faudra examiner quelles dispositions sur la protection des données instituées par des lois spéciales devront être conservées et lesquelles devront être adaptées en matière de traitement des données de personnes morales. Une disposition transitoire, à l'art. 71 nLPD, prévoit à cet effet que, pour les organes fédéraux, les dispositions d'autres actes de droit fédéral qui font référence à des données personnelles continuent de s'appliquer pendant les cinq ans suivant l'entrée en vigueur de la nLPD. Durant cette période, l'OFJ coordonnera la vérification et l'adaptation des bases légales concernant les données des personnes morales contenues dans des lois spéciales. Certaines dispositions sur les données des personnes morales ont déjà été modifiées dans le cadre de la révision totale de la LPD pour des raisons de praticabilité et de sécurité juridique. Pour ces cas, il faut procéder aux adaptations nécessaires dans les ordonnances. Le Conseil fédéral a décidé d'adopter une approche prudente. Pour cette raison, toutes les dispositions concernant les données des personnes morales qui apparaissent dans des ordonnances adoptées sur la base d'une loi sectorielle ne seront pas modifiées. Cette prudence vise à éviter de créer des conflits de droit, parce que certaines ordonnances seraient adaptées, mais que ces ordonnances se fondent sur d'autres lois sectorielles dans lesquelles les dispositions concernant les données des personnes morales figurant à l'annexe 1/II de la nLPD n'ont pas (encore) été modifiées. Une distinction est faite entre les ordonnances relatives à la LOGA et les autres lois sectorielles. Dans la LOGA, les dispositions concernant le traitement de données dans un système de gestion des affaires (art. 57h à h^{ter} LOGA) et l'utilisation de l'infrastructure électronique (art. 57i à 57l LOGA) sont modifiées. Une adaptation analogue doit être faite au niveau des ordonnances : elle doit se limiter aux ordonnances qui portent sur les mêmes aspects réglementaires. En outre, on renonce pour les motifs évoqués ci-dessus à adapter les ordonnances qui se fondent sur d'autres

⁵⁰ Voir les explications du Message du 15 septembre 2017 concernant la LPD (FF 2017 6565, 6643 s.).

⁵¹ Voir les explications du Message du 15 septembre 2017 concernant la LPD (FF 2017 6565, 6595, 6632 s.).

lois sectorielles qui n'ont pas été modifiées dans le cadre de la révision totale de la LPD. Dans les autres lois (p. ex. LTrans, loi sur la Banque nationale suisse), on adopte une approche globale. Pour une solution cohérente dans l'ensemble du domaine, seules les ordonnances qui se fondent sur une loi adaptée sont modifiées. Les dispositions d'une ordonnance subissent en outre des modifications lorsqu'elles sont nécessaires en termes de contenu (p. ex. parce qu'il s'agit d'une clarification ou de la mise en œuvre d'une disposition d'une loi qui est elle-même adaptée). La disposition transitoire de l'art. 71 nLPD selon laquelle le terme de « données personnelles » continue de s'appliquer au traitement des données des personnes morales et physiques, s'appliquera dans tous les cas pour les ordonnances qui ne sont pas adaptées. Les ordonnances suivantes sont modifiées dans l'annexe de l'OPDo :

- Ordonnance du 24 mai 2006 sur la transparence⁵² (voir ch. 7.15),
- Ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération⁵³ (voir ch. 7.18),
- Ordonnance du 30 juin 1993 concernant l'organisation de la statistique fédérale⁵⁴ (voir ch. 7.53),
- Ordonnance du 30 juin 1993 sur les relevés statistiques⁵⁵ (voir ch. 7.54),
- Ordonnance du 25 juin 2003 sur les émoluments et indemnités perçus pour les prestations de services statistiques des unités administratives de la Confédération⁵⁶ (voir ch. 7.56)
- Ordonnance du 9 juin 2017 sur le Registre fédéral des bâtiments et des logements⁵⁷ (voir ch. 7.57),
- Ordonnance du 30 juin 1993⁵⁸ sur le Registre des entreprises et des établissements (voir ch. 7.58),
- Ordonnance du 1^{er} novembre 2017 sur l'énergie⁵⁹ (voir ch. 7.76),
- Ordonnance du 14 mars 2008 sur l'approvisionnement en électricité⁶⁰ (voir ch. 7.79),
- Ordonnance du 6 septembre 2006 sur le travail au noir⁶¹ (voir ch. 7.114).

Enfin, les dispositions des ordonnances sectorielles sont aussi adaptées en fonction des nouveautés apportées par l'OPDo afin qu'il n'y ait pas de contradictions au moment de l'entrée en vigueur de l'ordonnance. On peut par exemple citer la modification de l'art. 4, al. 5, OPDo d'après lequel les procès-verbaux de journalisation devront être conservés séparément du système dans lequel les données personnelles sont traitées. En revanche, la durée de conservation des procès-verbaux dans les ordonnances sectorielles reste la même que prévu dans le droit en vigueur. Quant aux modalités du droit d'accès, les dispositions de droit sectoriel ont été adaptées afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande. L'ajout, selon lequel la personne doit prouver son identité a été supprimé dans les dispositions sectorielles, car cette exigence est désormais réglée à l'art. 16, al. 5, OPDo et qu'une précision dans le droit sectoriel ne semble pas nécessaire.

⁵² RS 152.31

⁵³ RS 172.010.442

⁵⁴ RS 431.011

⁵⁵ RS 431.012.1

⁵⁶ RS 431.09

⁵⁷ RS 431.841

⁵⁸ RS 431.903

⁵⁹ RS 730.01

⁶⁰ RS 734.71

⁶¹ RS 822.411

7.3 Ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes⁶²

Art. 12, al. 1, let. e, al. 2, let. a, ch. 2 et annexe 1, ch. 2.1, 2^e ligne

Selon l'art. 43, al. 1, nLPD, le préposé ne sera plus élu par le Conseil fédéral, mais par le Parlement. L'autorité chargée de l'élection doit décider si le préposé devra encore se soumettre à un contrôle de sécurité. C'est pourquoi la mention du préposé a été biffée à l'art. 12, al. 1, let. e et al. 2, let. a, ch. 2 ainsi qu'à l'annexe 1, ch. 2.1. Cependant, toutes les fonctions au sein du PFPDT, à l'exception du chef du PFPDT, sont soumises à un contrôle de sécurité. L'annexe 1, point 2.1, a été adaptée en conséquence

Art. 21, al. 2

Il s'agit d'adapter le renvoi conformément à la nouvelle numérotation de la nLPD.

7.4 Ordonnance du 4 décembre 2009 sur les mesures de police administrative de l'Office fédéral de la police et sur le système d'information HOOGAN⁶³

Art. 9, al. 1, let. a, ch. 3 et al. 4, let. b

L'expression « le préposé de fedpol à la protection des données et à la protection des informations » est remplacée par « le conseiller à la protection des données de fedpol ».

Art. 13, al. 1, let. a

Il s'agit d'adapter le renvoi à l'OPDo. Le renvoi à l'art. 20 OLPD est remplacé par un renvoi aux art. 1 à 4 et 6 OPDo car les dispositions relatives à la sécurité des données de la section 1 forment un ensemble. Le renvoi porte aussi sur les articles relatifs au règlement de traitement, qui sont inclus dans la section sur la sécurité des données.

7.5 Ordonnance du 16 août 2017 sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération⁶⁴

Art. 13, al. 1, let. a

Il s'agit d'adapter le renvoi à l'OPDo. Le renvoi à l'art. 20 OLPD est remplacé par un renvoi aux art. 1 à 4 et 6 OPDo car les dispositions relatives à la sécurité des données de la section 1 forment un ensemble. Le renvoi porte aussi sur les articles relatifs au règlement de traitement, qui sont inclus dans la section sur la sécurité des données.

Art. 17, al. 3, 23, al. 3, 30, al. 3 et 67, al. 2

Conformément à la modification apportée à l'art. 44, al. 1 LRens (annexe 1/II, ch. 2, nLPD), la notion de « données sensibles et profils de la personnalité » est remplacée par l'expression « données personnelles, sensibles ou non, y compris des données personnelles qui permettent d'évaluer la menace qu'une personne représente ».

⁶² RS 120.4

⁶³ RS 120.52

⁶⁴ RS 121.2

Art. 38, al. 1, 44, al. 1, 59, al. 1

Cette modification ne concerne que les textes français et italien. Le terme « fichier » est remplacé par celui de « données des dossiers ».

7.6 Ordonnance du 24 octobre 2007 relative à l'admission, au séjour et à l'exercice d'une activité lucrative⁶⁵

Art. 89a

Cette disposition subit deux modifications. D'une part, le renvoi à la loi sur les étrangers se réfère dorénavant à l'art. 111d, al. 3 et non plus à l'art. 111d dans son entier. D'autre part, l'art. 89a est modifié afin de respecter la terminologie de l'art. 16 nLPD et les garanties appropriées prévues aux art. 9 à 12 OPDo.

7.7 Ordonnance du 10 novembre 2021 sur le système d'entrée et de sortie⁶⁶

Art. 18, al. 1 et 20, al. 2, let. a

Il s'agit d'adapter les renvois à la nLPD et à l'OPDo.

7.8 Ordonnance 3 du 11 août 1999 sur l'asile⁶⁷

Art. 1b, al. 2, 1^{ère} phrase

Il s'agit de supprimer la notion de "profil de la personnalité".

Art. 6a

L'art. 6a est modifié afin de respecter la terminologie de l'art. 16 nLPD et les garanties appropriées prévues aux art. 9 à 12 OPDo.

Art. 12, let. a

Il s'agit d'adapter le renvoi à l'OPDo.

7.9 Ordonnance VIS du 18 décembre 2013⁶⁸

Art. 31, al. 1

La disposition est adaptée afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès et à la nLPD pour le droit à la rectification et à l'effacement.

Art. 32, al. 1, phrase introductive, let. a et c

La formulation de la phrase introductive a été légèrement modifiée sur la forme. Dans la lettre a, la notion de « maître du fichier » est remplacée par le terme « responsable du traitement ».

⁶⁵ RS 142.201

⁶⁶ RS 142.206

⁶⁷ RS 142.314

⁶⁸ RS 142.512

Comme pour la lettre c, la lettre a a également été adaptée pour correspondre à l'art. 19, al. 2, nLPD.

Art. 34, let. a

Il s'agit d'adapter le renvoi à l'OPDo.

7.10 Ordonnance SYMIC du 12 avril 2006⁶⁹

Art. 13, al. 1 phrase introductive et al. 4

Le terme « fichiers électroniques » est remplacé par « banques de données ». Cette modification ne concerne que le français.

Art. 14, al. 2

L'al. 2 est abrogé dans la mesure où il est en contradiction avec l'art. 39 nLPD.

Art. 17, al. 1, let. a

Il s'agit d'adapter le renvoi à l'OPDo.

Art. 19, al. 1 et 2

Le renvoi à la nLPD est adapté à l'al. 1. Pour que le texte corresponde aux versions françaises et italiennes, l'expression allemande « besonders schützenswerte Personendaten » est remplacée par « Personendaten ». La formulation de l'article est adaptée pour correspondre aux dispositions de l'art. 20, al. 1, OPDo.

7.11 Ordonnance du 20 septembre 2002 sur les documents d'identité⁷⁰

Art. 40, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées. Le principe selon lequel les procès-verbaux doivent être conservés sous une forme répondant aux exigences de la révision est biffé afin d'uniformiser le droit sectoriel.

Art. 42, al. 1 et 3

La disposition est adaptée afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès. À l'al. 3, le renvoi à la nLPD est adapté.

Art. 43

Il s'agit d'adapter le renvoi à la nLPD.

⁶⁹ RS 142.513

⁷⁰ RS 143.11

7.12 Ordonnance du 14 novembre 2012 sur l'établissement de documents de voyage pour étrangers⁷¹

Art. 30, al. 1, 3 et 5

La disposition est adaptée afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès. Les renvois à la nLPD aux al. 3 et 5 sont adaptés.

7.13 Ordonnance du 2 novembre 2016 concernant la loi fédérale relative à la convention internationale pour la protection de toutes les personnes contre les disparitions forcées⁷²

Art. 10, al. 2

Il s'agit d'adapter le renvoi conformément à la nouvelle numérotation de la nLPD.

7.14 Ordonnance du 8 septembre 1999 sur l'archivage⁷³

Art. 12, al. 3, 1^{ère} phrase et art. 14, al. 1, 1^{ère} phrase

Il s'agit de supprimer la notion de « profils de la personnalité ».

Art. 26, al. 2

L'al. 2 est abrogé car il s'agit d'un renvoi caduc.

7.15 Ordonnance du 24 mai 2006 sur la transparence⁷⁴

Art. 12, al. 1, 2, 1^{ère} et 2^e phrase et 3, art. 12a, al. 1, phrase introductive et 2, art. 12b, al. 1, phrase introductive, let. b et c, et 4, art. 13, al. 1, 3 et 4, art. 13a, titre, art. 21, phrase introductive

Le Préposé fédéral à la protection des données et à la transparence (préposé [fonction]) est remplacé par Préposé fédéral à la protection des données et à la transparence (PFPDT [institution]). Les modifications à l'art. 12, al. 2, 1^{ère} et 2^e phrase et 3, art. 12b, al. 1, let. b et c, et art. 13, al. 3, ne concernent que la version allemande.

Art. 13, al. 3 et 4

Conformément aux modifications apportées à la LTrans (annexe 1/II, ch. 10, nLPD), le terme de « données personnelles » est remplacé par « données des personnes physiques et morales ». L'al. 4 est uniquement modifié dans la version allemande.

⁷¹ RS 143.5

⁷² RS 150.21

⁷³ RS 152.11

⁷⁴ RS 152.31

7.16 Ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration⁷⁵

Art. 27i

Il s'agit d'adapter le renvoi à la nLPD.

7.17 Ordonnance GEVER du 3 avril 2019⁷⁶

Préambule

Conformément aux modifications de la LOGA (annexe 1/II, ch. 13, nLPD), l'ordonnance GEVER se fonde sur l'art. 57h^{ter} LOGA. Le préambule est adapté en ce sens.

Art. 2, al. 3

Cet alinéa est adapté pour correspondre au nouvel art. 57h, al. 1, LOGA (voir. ch. 13 Annexe 1/II nLPD).

7.18 Ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération⁷⁷

Titre

Le titre de l'ordonnance est complété par le traitement des « données des personnes morales » conformément aux modifications de la LOGA (annexe 1/II, ch. 13, nLPD).

Art. 1, let. a et b

Dans la définition des termes de « données administrées » et de « données non administrées », les données personnelles sont complétées par « les données des personnes morales ».

Art. 10, al. 3

Il s'agit d'adapter l'art. 10, al. 3 car chaque organe fédéral devra en principe disposer d'un conseiller à la protection des données.

Art. 14

Le terme de « données personnelles » est remplacé par « données ».

⁷⁵ RS 172.010.1

⁷⁶ RS 172.010.441

⁷⁷ RS 172.010.442

7.19 Ordonnance du 25 novembre 2020 sur la transformation numérique et l'informatique⁷⁸

Art. 26, al. 2

Le terme de « profil de la personnalité » est supprimé.

7.20 Ordonnance du 19 octobre 2016 sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération⁷⁹

Art. 11, al. 2

Cette disposition peut être supprimée puisque la notion de « profil de la personnalité » n'existe plus dans la nLPD.

Art. 13, al. 4 et 18, al. 1, 2^e phrase

La nLPD supprime l'obligation du responsable du traitement de déclarer ses fichiers au PFPDT (art. 11a, LPD). Elle prévoit en son art. 12, al. 4 que l'organe fédéral responsable doit déclarer ses registres d'activités au PFPDT. L'art. 13, al. 4, let. b, est donc adapté de manière à ce que la déclaration soit désormais liée à l'art. 12, al. 4, nLPD.

Les renvois à l'OPDo sont en outre adaptés à l'art. 13, al. 4 et à l'art. 18, al. 1, 2^e phrase.

Art. 17, al. 2, et 26, al. 2

En vue d'uniformiser la terminologie, une modification est apportée aux versions allemandes et italiennes. Les termes de « Datenschutzverantwortliche », « Datenschutzverantwortlicher » et « responsabile della protezione dei dati » ont été remplacés par « Datenschutzberaterin », « Datenschutzberater » et « consulente per la protezione dei dati » (voir à ce sujet le message du 15 septembre 2017 concernant la révision totale de la LPD, FF 2017 6565, 6652).

Art. 25, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.21 Ordonnance du 20 juin 2018 sur le traitement des données dans le système de gestion des mandats du Service linguistique DFAE⁸⁰

Préambule

En raison des modifications de la LOGA (ch. 13, annexe 1/II nLPD), l'ordonnance se fonde désormais sur l'art. 57^{h^{ter}} LOGA. Le préambule est adapté en conséquence.

⁷⁸ RS 172.010.58

⁷⁹ RS 172.010.59

⁸⁰ RS 172.010.60

Art. 13, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.22 Ordonnance du 4 mai 2016 sur les émoluments de fedpol⁸¹

Art. 1, al. 1, let. d

Il s'agit d'adapter le renvoi à l'OPDo.

7.23 Ordonnance du 12 février 2020 sur les marchés publics⁸²

Art. 24, al. 2, 2^e phrase

Il s'agit d'adapter le renvoi à la nLPD.

7.24 Ordonnance du 29 octobre 2008 sur l'organisation de la Chancellerie fédérale⁸³

Art. 5a, al. 3, let. c, et 10, al. 1

L'abréviation PFPDT est introduite à l'art. 5a, al. 3, let. c puis reprise à l'art. 10, al. 1.

7.25 Ordonnance SIVIP du 18 novembre 2015⁸⁴

Art. 11, al. 1, let. a

Il s'agit d'adapter le renvoi à l'OPDo.

7.26 Ordonnance du 25 novembre 1998 concernant l'Etat-major « Prise d'otage et chantage »⁸⁵

Art. 14, titre, al. 1, 1^{ère} phrase, et al. 2, 1^{ère} phrase

Dans le titre et à l'al. 1, il s'agit de remplacer le terme « fichier » par celui de « banque de données ». En raison de l'abrogation de la notion de « maître du fichier », l'al. 2 doit être adapté.

7.27 Ordonnance du 22 novembre 2017 concernant la protection des données personnelles du personnel de la Confédération⁸⁶

Art. 2

Il s'agit de remplacer le terme « fichier » par celui de « banque de données ».

⁸¹ RS 172.043.60

⁸² RS 172.056.11

⁸³ RS 172.210.10

⁸⁴ RS 172.211.21

⁸⁵ RS 172.213.80

⁸⁶ RS 172.220.111.4

Art. 9, al. 1

La notion de « profil de la personnalité » est supprimée.

Art. 34, al. 1, let. b

La nLPD supprime l'obligation du responsable du traitement de déclarer ses fichiers au PFPDT (art. 11a LPD). Elle prévoit en son art. 12, al. 4 que l'organe fédéral responsable doit déclarer ses registres d'activités au PFPDT. L'art. 34, al. 1, let. b est adapté de façon à ce que la communication se fonde sur l'art. 12, al. 4, nLPD.

Art. 16, al. 2, 28, al. 2, 37, al. 2, 44, al. 2, 51, al. 2, 57, al. 2, et 65, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.28 Ordonnance Web-DFAE du 5 novembre 2014⁸⁷

Préambule

En raison des modifications de la LOGA (ch. 13, annexe 1/II nLPD), l'ordonnance se fonde désormais sur l'art. 57^{h^{ter}} LOGA. Le préambule est adapté en conséquence.

Art. 12, al. 1, let. a

Il s'agit d'adapter le renvoi à l'OPDo.

Art. 13, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées. La durée de conservation a été adaptée à la durée minimale de l'art. 4, al. 5, OPDo.

7.29 Ordonnance du 28 avril 2004 sur l'état civil (OEC)⁸⁸

Art. 83, al. 2 à 4

Les modifications de l'art. 83, al. 2 à 4, OEC permettent de remplir le mandat législatif de l'art. 45a, al. 5, ch. 5 du code civil (modifié dans le cadre de la nLPD). Celui-ci charge le Conseil fédéral de régler, en collaboration avec les cantons, la surveillance du respect des dispositions de protection des données dans le registre de l'état civil. Le principe selon lequel les registres publics relatifs aux rapports de droit privé sont exclus de la LPD est abandonné en vertu de l'art. 2, al. 4, nLPD. Le registre de l'état civil est dès lors soumis à la surveillance du PFPDT en ce qui concerne le respect des dispositions de protection des données (art. 4, al. 2, nLPD, a contrario). L'al. 2 prévoit, pour coordonner cette surveillance, que l'Office fédéral de l'état civil (OFEC) invite le PFPDT à prendre position avant de prendre une mesure concernant des questions de protection et de sécurité des données. Si le PFPDT agit dans le cadre de sa surveillance, il devra, selon l'al. 4, assurer la coordination avec l'OFEC et les

⁸⁷ RS 172.220.111.42

⁸⁸ RS 211.112.2

autorités cantonales de protection des données. L'al. 3 correspond quant à lui à l'art. 83, al. 2, OEC.

7.30 Ordonnance du 18 novembre 1992 sur la mensuration officielle⁸⁹

Art. 40, al. 5

La tenue d'un registre de données est remplacée par le traitement des données.

7.31 Ordonnance du 17 octobre 2007 sur le registre du commerce⁹⁰

Art. 12c, al. 2

Dans les versions françaises et italiennes, le terme de « fichiers » est remplacé par « banques de données ».

7.32 Ordonnance Ordipro du 22 mars 2019⁹¹

Art. 15, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.33 Ordonnance E-VERA du 17 août 2016⁹²

Art. 9, titre, al. 1, phrase introductive

Dans la version française, la modification porte sur la suppression du terme « fichier ». Dans les versions allemande et italienne, il s'agit de remplacer les termes « Datensatz », respectivement « set di dati » par « Daten », respectivement « dati ». Dans les trois versions, des adaptations grammaticales sont en outre nécessaires.

Art. 14, al. 1, let. a

Il s'agit d'adapter le renvoi à l'OPDo.

Art. 15, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

⁸⁹ RS 211.432.2

⁹⁰ RS 221.411

⁹¹ RS 235.21

⁹² RS 235.22

7.34 Ordonnance CV-DFAE du 26 avril 2017⁹³

Art. 6, titre

La modification ne concerne que le texte allemand. Le terme « Datensatz » est remplacé par « Daten » pour que la terminologie soit uniforme dans toutes les ordonnances sur les systèmes d'information du DFAE (voir art. 9, al. 1, de l'ordonnance E-VERA).

Art. 11, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.35 Ordonnance « e-vent » du 17 octobre 2018⁹⁴

Préambule

En raison des modifications de la LOGA (ch. 13, annexe 1/II nLPD), l'ordonnance se fonde désormais sur l'art. 57^{h^{ter}} LOGA. Le préambule est adapté en conséquence.

Art. 13, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.36 Ordonnance Plato du 25 septembre 2020⁹⁵

Préambule

En raison des modifications de la LOGA (ch. 13, annexe 1/II nLPD), l'ordonnance se fonde désormais sur l'art. 57^{h^{ter}} LOGA. Le préambule est adapté en conséquence.

Art. 14, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.37 Ordonnance du 26 juin 2013 sur la Commission fédérale chargée de juger les possibilités de traiter les personnes internées à vie⁹⁶

Art. 13, al. 1

Il s'agit d'adapter le renvoi à la nLPD.

⁹³ RS 235.23

⁹⁴ RS 235.25

⁹⁵ RS 235.26

⁹⁶ RS 311.039.2

7.38 Ordonnance du 7 novembre 2012 sur la protection extraprocédurale des témoins⁹⁷

Art. 13, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

Art. 15, al. 1, let. b

Il s'agit d'adapter le renvoi à l'OPDo.

7.39 Ordonnance du 20 septembre 2013 relative au système d'information en matière pénale de l'Office fédéral de la douane et de la sécurité des frontières⁹⁸

Art. 3

Il s'agit d'adapter le renvoi conformément à la nouvelle numérotation de l'OPDo.

Art. 14, al. 1 et 2

À l'al. 1, il s'agit d'adapter le renvoi conformément à la nouvelle numérotation de la nLPD.

La révision de la loi fédérale du 22 mars 1974 sur le droit pénal administratif⁹⁹ (voir annexe 1/II, ch. 27, nLPD), introduit un nouvel art. 18d qui règle le droit aux renseignements des parties et des autres participants à une procédure pendante. Il y a lieu par conséquent de mentionner l'art. 18d à l'al. 2.

Art. 18, al. 1

Le renvoi aux art. 20 et 21 OLPD est remplacé par un renvoi aux art. 1 à 4 et 6 OPDo.

7.40 Ordonnance VOSTRA du 29 septembre 2006¹⁰⁰

Art. 18, al. 5

Il s'agit de remplacer le terme « fichier » par celui de « banque de données ».

Art. 26, al. 1, 2^e phrase, 2 et 4

Il s'agit d'adapter les renvois conformément à la nouvelle numérotation de la nLPD. L'al. 2 est adapté afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès.

Art. 27, al. 1, let. b

Il s'agit d'adapter le renvoi à la nouvelle numérotation de l'OPDo.

⁹⁷ RS 312.21

⁹⁸ RS 313.041

⁹⁹ RS 313.0

¹⁰⁰ RS 331

Art. 32

Il s'agit d'adapter le renvoi conformément à la nouvelle numérotation de la nLPD. L'article est aussi adapté à la terminologie de l'art. 39 nLPD.

7.41 Ordonnance GPDA du 23 septembre 2016¹⁰¹

Préambule

En raison des modifications de la LOGA (ch. 13, annexe 1/II nLPD), l'ordonnance se fonde désormais sur l'art. 57^hter LOGA. Le préambule est adapté en conséquence.

Art. 14, al. 1, phrase introductive et let. a

Il s'agit d'adapter le renvoi à la nouvelle législation sur la protection des données. La modification de la phrase introductive ne concerne que la version française, qui est adaptée pour correspondre aux textes allemand et italien. Le terme « sécurité informatique » est remplacé par celui de « sécurité des données ».

Art. 15, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées. Afin d'uniformiser le droit sectoriel, « à compter de la date de leur établissement » est biffé.

Art. 17

Il s'agit d'adapter le renvoi à la nLPD.

7.42 Ordonnance du 30 novembre 2001 concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police¹⁰²

Art. 6, al. 1, let. c et d, et 2, let. b et c

Il s'agit d'adapter la formulation car l'art. 13, al. 2 de 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 États (LOC ; RS 360) ne contient plus de conditions mais renvoie à des dispositions du code pénal.

7.43 Ordonnance JANUS du 15 octobre 2008¹⁰³

Art. 19, al. 1, let. a et b, et 2, let. a et b

Il s'agit d'adapter la formulation car l'art. 13, al. 2, LOC ne contient plus de conditions mais renvoie à des dispositions du code pénal.

¹⁰¹ RS 351.12

¹⁰² RS 360.1

¹⁰³ RS 360.2

Art. 24, al. 1, et 26

Il s'agit d'adapter les renvois à la nLPD et à la nouvelle numérotation de l'OPDo.

Art. 26, let. a, 29l, 2^e phrase, 29n, al. 1, let. a, 29v, al. 1, 2^e phrase, et 29w, al. 1, let. a

Il s'agit d'adapter les renvois à la nouvelle législation sur la protection des données.

Art. 27, al. 1, 2^e phrase, 29i, al. 2, et 29t, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

Annexe 2, ch. 4.1, 1^{ère} ligne, 2^e colonne

Le terme de « fichier » est remplacé par « banque de données ».

7.44 Ordonnance RIPOL du 26 octobre 2016¹⁰⁴

Art. 2, al. 1, phrase introductive et let. f, 13, al. 1 et 14, al. 2, let. a

À l'art. 2, al. 1, 1^{ère} phrase, La notion de « maître du fichier » est remplacée par celle d'« organe fédéral ». Les autres modifications correspondent à une adaptation des renvois à la nouvelle législation sur la protection des données.

Art. 13, al. 1^{bis} et 2

La révision de la loi du 13 juin 2008 sur les systèmes d'information de police de la Confédération¹⁰⁵ (voir annexe 1/II, ch. 30, nLPD) prévoit un nouvel art. 8a LSIP qui introduit une restriction du droit d'accès aux signalements en vue d'une arrestation aux fins d'extradition qui figurent dans un des systèmes énumérés à l'art. 2 de cette loi, notamment le système de recherches informatisées de police (RIPOL). Il y a lieu par conséquent de mentionner l'art. 8a dans un nouvel al. 1^{bis} à l'art. 13.

L'al. 2 est adapté afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès.

Art. 15, al. 1, 2^e phrase et 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.45 Ordonnance IPAS du 15 octobre 2008¹⁰⁶

Art. 9a et 13, 2^e phrase

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

¹⁰⁴ RS 361.0

¹⁰⁵ RS 361

¹⁰⁶ RS 361.2

La modification de l'art. 9a, 2^e phrase, ne concerne que les versions allemande et italienne : le terme « *Datenschutzbeauftragten* » est remplacé par « *Datenschutzberaterin* » et « *Datenschutzberater* ».

Art. 10 et 12

Les renvois à la nouvelle législation fédérale sur la protection des données doivent être adaptés.

7.46 Ordonnance du 6 décembre 2013 sur le traitement des données signalétiques biométriques¹⁰⁷

Art. 3, al. 1, let. b et d

Les modifications concernent uniquement les textes français et italien. Il s'agit de remplacer le terme de « fichier » par celui de « registre ».

Art. 3a, 2^e phrase, 6 et 14, let. a

Les renvois à la nouvelle législation sur la protection des données doivent être adaptés.

Art. 5, al. 2

La disposition est adaptée afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès.

7.47 Ordonnance du 15 octobre 2008 sur l'index national de police¹⁰⁸

Art. 7, al. 1 et 12, al. 1

Les renvois à la nouvelle législation sur la protection des données doivent être adaptés.

Art. 8, al. 1, let. c et d

Les renvois à l'ordonnance RIPOL¹⁰⁹ du 15 octobre 2008 et à l'ordonnance N-SIS¹¹⁰ du 7 mai 2008 sont actualisés.

Art. 11, al. 1 et 2, phrase introductive et 3

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées. Les modifications à l'al. 1 et 2 ne concernent que la version allemande. Le terme de « *Datenschutzbeauftragten* » est remplacé par « *Datenschutzberaterin* » et « *Datenschutzberater* ».

¹⁰⁷ RS 361.3

¹⁰⁸ RS 361.4

¹⁰⁹ RS 361.0

¹¹⁰ RS 362.0

7.48 Ordonnance N-SIS du 8 mars 2013¹¹¹

Art. 50, al. 1

La disposition est adaptée afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès et à la nLPD pour le droit à la rectification et à l'effacement. Dans le titre et à l'al. 1 des versions française et italienne, « droit à l'information » a été remplacé par « droit d'accès » afin de correspondre à la version allemande.

Art. 50, al. 6

La révision de la loi du 13 juin 2008 sur les systèmes d'information de police de la Confédération¹¹² (voir annexe 1/II, ch. 30, nLPD) prévoit un nouvel art. 8a LSIP qui introduit une restriction du droit d'accès aux signalements en vue d'une arrestation aux fins d'extradition qui figurent dans un des systèmes énumérés à l'art. 2 de cette loi, notamment le système d'information Schengen. Il y a lieu par conséquent de mentionner l'art. 8a dans un nouvel alinéa 6 à l'art. 50.

Art. 51, al. 1 et 2, let. c et 53, al. 1, let. a

Les renvois à la nouvelle législation sur la protection des données doivent être adaptés.

7.49 Ordonnance du 3 décembre 2004 sur les profils d'ADN¹¹³

Art. 8, al. 1

La notion de « maître » est remplacée par les termes « organe fédéral responsable ». La seconde partie de la phrase de l'al. 1 peut être supprimée.

Art. 17, al. 1 et 3, 1^{ère} phrase, et 19, al. 1, let. a

Il s'agit d'adapter le renvoi à la numérotation de la nLPD, respectivement de l'OPDo. La formulation de l'art. 17, al. 3 est adaptée, car l'art. 62 nLPD n'édicte pas directement un devoir de discrétion, mais uniquement les conséquences qui se produisent en cas de violation de ce devoir.

À l'art. 19, al. 1, les renvois aux art. 20 à 23 OLPD sont remplacés par un renvoi aux art. 1 à 4 et 6 OPDo, dans la mesure où la réglementation de l'art. 19 ne concerne, selon son intitulé, que le domaine de la sécurité des données. Les dispositions de l'OPDo relatives à la sous-traitance et au conseiller à la protection des données trouvent également application.

¹¹¹ RS 362.0

¹¹² RS 361

¹¹³ RS 363.1

7.50 Ordonnance Interpol du 21 juin 2013¹¹⁴

Art. 4, al. 1, let. f, 11, al. 4, 3^e phrase, 12, al. 2, 2^e phrase, 16, al. 1, 17, al. 1

L'expression « le conseiller à la protection des données et des informations de fedpol » est remplacée par « le conseiller à la protection des données de fedpol » (voir les commentaires dans le message concernant la révision totale de la LPD, FF 2017 6565, 6652 s.).

Art. 16, al. 1 et 7

L'al. 1 est adapté afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès. L'al. 7 se réfère à la nLPD pour le droit à la rectification et à l'effacement.

7.51 Ordonnance du 15 septembre 2017 sur les systèmes d'information dans le domaine de la formation professionnelle et des hautes écoles¹¹⁵

Art. 20 et 21, al. 1, let. a

Il s'agit d'adapter le renvoi à la nLPD.

7.52 Ordonnance du 29 novembre 2013 sur l'encouragement de la recherche et de l'innovation¹¹⁶

Art. 41a, al. 3

Il s'agit de supprimer la notion de « profil de la personnalité » est d'adapter le renvoi à la numérotation de la nLPD.

7.53 Ordonnance du 30 juin 1993 concernant l'organisation de la statistique fédérale¹¹⁷

Art. 9, al. 1, 2^e phrase, et 4

Pour que les autres versions linguistiques correspondent au français, le terme de « administrative Datensammlungen » a été remplacé par « Beständen von administrativen Daten » et un changement équivalent a été apporté à la version italienne.

Art. 10

Le renvoi à la législation sur la protection des données doit être adapté. Selon l'art. 16 de la loi sur la statistique fédérale (LSF ; annexe 1/II, ch. 35, nLPD), le renvoi à l'al. 1 n'est valable que pour les données personnelles. L'al. 2, qui concerne la sécurité des données, porte quant à lui tant sur les données personnelles que sur les données des personnes morales, conformément à l'art. 15, al. 1, LSF. D'après le message concernant la modification de la LPD (FF 2017 6565, 6747), le principe de la sécurité des données doit valoir pour les deux catégories de personnes.

¹¹⁴ RS 366.1

¹¹⁵ RS 412.108.1

¹¹⁶ RS 420.11

¹¹⁷ RS 431.011

7.54 Ordonnance du 30 juin 1993 sur les relevés statistiques¹¹⁸

Art. 5, al. 2, phrase introductive et 3

L'expression « des données se référant à des personnes » est remplacée par « des données personnelles et des données des personnes morales » à l'art. 5, al. 2. À l'al. 3, le texte en français est adapté à la terminologie en allemand (« mesures d'organisation » est remplacé par « mesures techniques et organisationnelles »). Le renvoi de l'al. 3 est adapté de façon à ce que les dispositions concernant la sécurité des données des personnes morales s'appliquent par analogie (voir explications au ch. 7.53).

Art. 13m, al. 1

En raison de l'abrogation de la notion de « profil de la personnalité », l'art. 14a de la loi fédérale du 9 octobre 1992 sur la statistique fédérale¹¹⁹ relatif à l'appariement des données a été modifié (voir ch. 35 de l'annexe 1/II, nLPD). La notion de « profils de la personnalité » a ainsi été remplacée par les termes « les caractéristiques essentielles d'une personne physique ou morale ». La même modification doit être effectuée à l'art. 13m, al. 1.

Annexe

Dans toute l'annexe, « fichier suisse des étudiants du SIUS » est remplacé par « banque de données suisse des étudiants du SIUS » et « fichier suisse du personnel des hautes écoles » est remplacé par « banque de données suisse du personnel des hautes écoles », et les adaptations grammaticales nécessaires qui en découlent ont été effectuées

7.55 Ordonnance du 26 janvier 2011 sur le numéro d'identification des entreprises¹²⁰

Art. 3, al. 1, let. b et d, 8, al. 4 et 20, al. 3

Il s'agit de remplacer l'expression « fichier de données » par celle de « banque de données ».

7.56 Ordonnance du 25 juin 2003 sur les émoluments et indemnités perçus pour les prestations de services statistiques des unités administratives de la Confédération¹²¹

Art. 1, let. d

Le terme de « données personnelles » est remplacé par « données personnelles et données des personnes morales ».

¹¹⁸ RS 431.012.1

¹¹⁹ RS 431.01

¹²⁰ RS 431.031

¹²¹ RS 431.09

7.57 Ordonnance du 9 juin 2017 sur le Registre fédéral des bâtiments et des logements¹²²

Art. 9, al. 2, let. f

Cette modification ne concerne que le texte allemand. Il s'agit de remplacer le terme « Datensammlung » par « Datenbank ».

Art. 18, al. 1, let. a et 2

Il s'agit d'adapter le renvoi à l'OPDo. Dans le domaine des statistiques, les dispositions concernant la sécurité des données des personnes morales s'appliquent par analogie (voir explications au ch. 7.53).

7.58 Ordonnance du 30 juin 1993 sur le Registre des entreprises et des établissements¹²³

Art. 9a, al. 2, 10, al. 3, 14, al. 1 et 15, let. a

Il s'agit d'adapter les renvois à la nLPD et à l'OPDo.

Art. 15, al. 2

Dans le domaine des statistiques, les dispositions concernant la sécurité des données des personnes morales s'appliquent par analogie (voir explications au ch. 7.53).

7.59 Ordonnance du 4 septembre 2013 sur la circulation des espèces de faune et de flore protégées¹²⁴

Art. 54

Le renvoi à la nLPD est adapté à l'al. 1. L'al. 2 renvoie à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès.

7.60 Ordonnance animex-ch du 1^{er} septembre 2010¹²⁵

Art. 18, al. 1 et 2

Il s'agit à l'al. 1 d'adapter le renvoi à la nLPD. L'al. 2 est adapté afin de renvoyer à l'art. 16 OPDo en ce qui concerne la demande d'accès.

7.61 Ordonnance du 4 décembre 2009 concernant le Service de renseignement de l'armée¹²⁶

Art. 8, titre et phrase introductive

En raison de l'abrogation de la notion de « profil de la personnalité », cette disposition doit être modifiée. De manière conforme à l'art. 99, al. 2, LAAM, il s'agit d'introduire les termes

¹²² RS 431.841

¹²³ RS 431.903

¹²⁴ RS 453.0

¹²⁵ RS 455.61

¹²⁶ RS 510.291

« y compris les données sensibles ou non et d'autres données personnelles qui permettent d'évaluer la menace qu'une personne représente » (voir le ch. 40 de l'annexe 1/II, nLPD).

Art. 9

La nLPD prévoit à son art. 56 que le PFPDT tient un registre public des activités de traitements que les organes fédéraux lui ont préalablement annoncés (art. 12, al. 4 nLPD), et non plus un registre des fichiers (art. 11a, al. 1, LPD). Selon l'art. 99, al. 3, let. d de la loi sur l'armée (LAAM ; annexe 1/II, ch. 40, nLPD), le Conseil fédéral règle les exceptions à l'enregistrement des activités de traitement des données lorsque, à défaut, la recherche des informations serait compromise. L'art. 9, al. 1, prévoit que les activités de traitement qui sont effectuées dans le cadre d'une acquisition de renseignements conformément à l'art. 99, al. 2, LAAM ne doivent pas être déclarées au PFPDT, si l'acquisition de renseignements est mise en péril de ce fait. Selon l'al. 2, le Service de renseignement de l'armée (SRA) doit donner des informations générales à propos de ces activités de traitement au PFPDT.

Art. 10, al. 2

Les termes « fichier de données indépendants » sont remplacés par « banque de données indépendante ».

7.62 Ordonnance du 17 octobre 2012 sur la guerre électronique et l'exploration radio¹²⁷

Art. 4, al. 5

L'obligation d'enregistrer les fichiers est remplacée par la déclaration des registres d'activité de traitement.

7.63 Ordonnance du 4 juillet 2007 concernant la protection des informations¹²⁸

Art. 3, let. h

Le terme de « fichiers de données » est remplacé par « banques de données ». D'autres petites modifications sont apportées au texte français pour qu'il corresponde à celui des autres langues.

7.64 Ordonnance du 21 mai 2008 sur la géoinformation (OGéo)¹²⁹

Dans toute l'ordonnance

La modification ne concerne que l'allemand. Le terme « Datensammlung » est remplacé par celui de « Daten ».

Art. 3a

L'art. 11, al. 2 de la loi du 5 octobre 2007 sur la géoinformation (LGéo)¹³⁰ a été modifié dans le cadre de la révision totale de la LPD. D'après cet article, le Conseil fédéral peut prévoir

¹²⁷ RS 510.292

¹²⁸ RS 510.411

¹²⁹ RS 510.620

¹³⁰ RS 510.62

des exceptions à l'obligation de tenir un registre des activités de traitement lorsque les traitements présentent un risque limité d'atteinte aux droits fondamentaux de la personne concernée. Le catalogue des géodonnées de l'annexe 1 de l'OGéo concerne actuellement peu de données personnelles et le traitement des données concernées ne présente aucun risque, ou un risque minime de porter atteinte aux droits fondamentaux des personnes, d'autant plus que la loi spéciale prévoit généralement explicitement la communication des données personnelles. Le catalogue des géodonnées de l'annexe 1 répond ainsi aux exigences de l'art. 11, al. 2, LGéo. À chaque fois qu'un élément est ajouté au catalogue, il faudra vérifier si les nouvelles données satisfont aux exigences.

7.65 Ordonnance du 16 décembre 2009 sur les systèmes d'information de l'armée¹³¹

Art. 2a, 2b, let. b, annexe 1, titre et 1^{ère} ligne, 4^e colonne

Il s'agit de supprimer les termes « maître du fichier ».

Titre précédant l'art. 72h, section 5, art. 72h, 72h^{bis}, 72h^{quater}, 72h^{quinquies}, annexe 35d, titre

La modification ne concerne que l'allemand : le terme « Hilfsdatensammlungen » est remplacé par « Hilfsdatenbanken ».

7.66 Ordonnance du 21 novembre 2018 sur la sécurité militaire¹³²

Art. 4, al. 3

Il s'agit d'adapter le renvoi à la nLPD.

Art. 5

La nLPD prévoit à son art. 56 que le PFPDT tient un registre public des activités de traitements que les organes fédéraux lui ont préalablement annoncés (art. 12, al. 4 nLPD), et non plus un registre des fichiers (art. 11a, al. 1, LPD). Selon l'art. 100, al. 4, let. c, ch. 2, LAAM (annexe 1/II, ch. 40, nLPD), le Conseil fédéral règle les exceptions à l'obligation de déclarer les registres des activités de traitement au PFPDT pour enregistrement si cela compromet la recherche d'informations. De ce fait, l'art. 5 prévoit que les activités de traitement effectuées dans le cadre d'un service d'appui ou d'un service actif ne doivent pas être annoncées au PFPDT si cela compromet la recherche d'informations et l'accomplissement des tâches prévues par cette ordonnance. En application de l'al. 2, le SRA doit toutefois informer le PFPDT de façon générale sur ces activités de traitement. Dans la version allemande du texte, la mention du PFPDT est adaptée afin qu'il soit clair que cet alinéa vise l'institution dans son ensemble et pas directement le préposé.

¹³¹ RS 510.911

¹³² RS 513.61

7.67 Ordonnance du 2 juillet 2008 sur les armes¹³³

Art. 58, al. 1, let. h, 59, al. 1, phrase introductive, 59a, al. 1 phrase introductive, 60, titre, 66a, 1^{ère} phrase, 66b, 66d, 68, al. 2, let. c, 69 let. c et 70, al. 1, let. c et al. 2, let. c

Seule la version française de ces dispositions est concernée. Il s'agit de remplacer le terme « fichier » par « banque de données ».

Art. 64

Cette disposition subit deux modifications. D'une part, le renvoi à la loi sur les armes se réfère dorénavant à l'art. 32e, al. 3 et non plus à l'art. 32e dans son entier. D'autre part, l'art. 64 est modifié afin de respecter la terminologie de l'art. 16 nLPD et les garanties appropriées prévues aux art. 9 à 12 OPDo.

Art. 65, 66b et 66c, al. 1, let. a

Il s'agit d'adapter les renvois à la nLPD, respectivement à l'OPDo.

Art. 66a, 2e phrase

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.68 Ordonnance du 11 novembre 2020 sur la protection civile¹³⁴

Art. 37, al. 3

Le terme « maître de données » est remplacé « responsable des données ».

7.69 Ordonnance du 12 août 2015 sur le bureau de notification pour les médicaments vitaux à usage humain¹³⁵

Art. 8, al. 2, let. a

Il s'agit d'adapter le renvoi à l'OPDo.

7.70 Ordonnance du 5 avril 2006 sur les finances de la Confédération¹³⁶

Art. 1, al. 2, et 26, al. 2

Le PFPDT dispose de sa propre compétence budgétaire en vertu de la nLPD. Selon l'art. 45 nLPD, il remet chaque année, par l'intermédiaire de la Chancellerie fédérale, son projet de budget au Conseil fédéral, puis celui-ci le transmet tel quel à l'Assemblée fédérale. Par conséquent, l'art. 142, al. 2 de la loi sur le Parlement (annexe 1/II, ch. 12, nLPD) prévoit que le Conseil fédéral reprend tels quels dans son projet de budget et dans le compte d'État les projets de budget et les comptes du PFPDT. Selon l'al. 3 de ce même article, le PFPDT défend son projet de budget et ses comptes devant l'Assemblée fédérale. Ces modifications sont

¹³³ RS 514.541

¹³⁴ RS 520.11

¹³⁵ RS 531.215.32

¹³⁶ RS 611.01

donc adaptées aux art. 1, al. 1, let. g et al. 2, et 26, al. 2 de l'ordonnance sur les finances de la Confédération.

7.71 Ordonnance du 1^{er} novembre 2006 sur les douanes¹³⁷

Art. 226, al. 3, let. b.

L'art. 103, al. 1, phrase introductive de révision de la loi sur les douanes (annexe 1/II, ch. 48, nLPD) habilite dorénavant l'Office fédéral de la douane et de la sécurité des frontières à établir l'identité d'une personne en relevant des données génétiques. La base légale prévue aujourd'hui à l'art. 226, al. 3, let. b, ch. 1 peut donc être supprimée (voir ch. 9.2.37 du message du Conseil fédéral du 15 septembre).

7.72 Ordonnance du 4 avril 2007 régissant l'utilisation d'appareils de prises de vue, de relevé et d'autres appareils de surveillance par l'Office fédéral de la douane et de la sécurité des frontières¹³⁸

Art. 10, al. 1

Il s'agit d'adapter le renvoi à la nLPD.

7.73 Ordonnance du 23 août 2017 sur le traitement des données dans l'OFDF¹³⁹

Préambule

En raison des modifications de la LOGA (ch. 13, annexe 1/II nLPD), l'ordonnance se fonde désormais sur l'art. 57^{h^{ter}} LOGA. Le préambule est adapté en conséquence.

Art. 8 et 12, al. 1

Il s'agit d'adapter le renvoi à la nLPD et à l'OPDo. À l'art. 12, le renvoi aux art. 20 et 21 OLPD est remplacé par un renvoi aux art. 1 à 4 et 6 OPDo.

Annexe 73

Cette modification ne concerne que le texte allemand. Le terme « Hilfsdatensammlungen » est remplacé par « Hilfsdatenbanken ».

7.74 Ordonnance du 12 octobre 2011 sur la statistique du commerce extérieur¹⁴⁰

Art. 13

Cette modification ne concerne que le texte allemand. Le terme « Datensammlungen » est remplacé par « Hilfsdatenbanken ».

¹³⁷ RS 631.01

¹³⁸ RS 631.053

¹³⁹ RS 631.061

¹⁴⁰ RS 632.14

7.75 Ordonnance du 27 novembre 2009 régissant la taxe sur la valeur ajoutée¹⁴¹

Art. 135, al. 2

Cette modification s'inscrit dans le cadre de l'adaptation de l'art. 14, al. 3 de la loi sur la Banque nationale¹⁴² visant à créer une base légale pour l'échange de données entre la BNS, l'Administration fédérale des contributions (AFC) et l'Office fédéral de la statistique (OFS) à des fins statistiques¹⁴³.

7.76 Ordonnance du 1^{er} novembre 2017 sur l'énergie¹⁴⁴

Art. 70

Comme dans la modification de la loi sur l'énergie (annexe 1/II, ch. 56, nLPD), les données personnelles sont complétées par les « données [concernant] des personnes morales ». Une autre modification terminologique ne concerne que l'allemand : « administrative und strafrechtliche Verfolgungen und Sanktionen » est remplacé par « verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen » conformément à l'art. 5, let. c, nLPD.

7.77 Ordonnance du 9 juin 2006 sur les qualifications du personnel des installations nucléaires¹⁴⁵

Art. 39, al. 1, phrase introductive

La notion de « profil de la personnalité » est supprimée.

7.78 Ordonnance du 9 juin 2006 sur les équipes de surveillance des installations nucléaires¹⁴⁶

Art. 18, al. 1

La notion de « profil de la personnalité » est supprimée.

7.79 Ordonnance du 14 mars 2008 sur l'approvisionnement en électricité¹⁴⁷

Art. 8d, al. 1, 2, let. a et 3

Le terme de « profils de la personnalité » est biffé. Conformément à la modification adoptée dans la loi sur l'approvisionnement en électricité (annexe 1/II, ch. 59, nLPD), le terme de données personnelles est complété par les « données des personnes morales ».

¹⁴¹ RS 641.201

¹⁴² RS 951.11

¹⁴³ Voir message du 15 septembre 2017 concernant la LPD (FF 2017 6565, 6762 s.)

¹⁴⁴ RS 730.01

¹⁴⁵ RS 732.143.1

¹⁴⁶ RS 732.143.2

¹⁴⁷ RS 734.71

Art. 8d, al. 5, 2e phrase

Il s'agit d'adapter le renvoi à l'OPDo. Conformément à la modification de l'art. 17c, al. 1 de la loi sur l'approvisionnement en électricité, les dispositions de l'OLPD concernant les données des personnes morales s'appliquent par analogie.

7.80 Ordonnance du 30 novembre 2018 sur le système d'information relatif aux accidents de la route¹⁴⁸

Préambule

Il s'agit d'adapter le renvoi à la nLPD.

Art. 17, al. 4

Il s'agit d'adapter le renvoi à la nLPD et à l'OPDo.

7.81 Ordonnance du 30 novembre 2018 sur le système d'information relatif à l'admission à la circulation¹⁴⁹

Préambule

Il s'agit d'adapter le renvoi à la nLPD.

Art. 18, al. 5

Il s'agit d'adapter le renvoi à l'OPDo.

7.82 Ordonnance du 4 novembre 2009 sur la vidéosurveillance dans les transports publics¹⁵⁰

Art. 6, al. 2

Le renvoi à l'OPDo doit être adapté.

7.83 Ordonnance du 17 décembre 2014 sur les enquêtes de sécurité en cas d'incident dans le domaine des transports¹⁵¹

Art. 19, al. 2

Le renvoi à la nLPD est adapté à l'al. 2.

Par ailleurs, une adaptation formelle est apportée dans la version française de façon à ce que l'article comporte deux alinéas, comme dans les autres versions linguistiques.

¹⁴⁸ RS 741.57

¹⁴⁹ RS 741.58

¹⁵⁰ RS 742.147.2

¹⁵¹ RS 742.161

7.84 Ordonnance du 2 septembre 2015 sur la licence d'entreprise de transport de voyageurs et de marchandises par route¹⁵²

Art. 14

La disposition est adaptée afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès et à la nLPD pour le droit à la rectification.

7.85 Ordonnance du 4 novembre 2009 sur le transport de voyageurs¹⁵³

Art. 58b, al. 1

La disposition est adaptée afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès et à la nLPD pour le droit à la rectification.

7.86 Ordonnance du 18 décembre 1995 sur le service de la navigation aérienne¹⁵⁴

Art. 40a, al. 1 et 2

À l'al. 1, « les prestataires de services » a été remplacé par le singulier « le prestataire de services » par souci de cohérence avec les alinéas suivants. À l'al. 2, les termes « fichier de données » sont remplacés par l'expression « banque de données ».

7.87 Ordonnance du 15 novembre 2017 surveillance de la correspondance par poste et télécommunication¹⁵⁵

Art. 8, al. 2

Le terme de « préposé à la protection des données » est remplacé par celui de « conseiller à la protection des données ».

7.88 Ordonnance du 15 novembre 2017 sur le système de traitement pour la surveillance de la correspondance par poste et télécommunication¹⁵⁶

Art. 7, al. 4, et 8, al. 2, 1^{ère} phrase

Il s'agit d'adapter le renvoi à l'OPDo et à la nLPD.

7.89 Ordonnance du 9 mars 2007 sur les services de télécommunication¹⁵⁷

Art. 48, al. 3, 2^e phrase

Cette modification ne concerne que le texte allemand. L'expression « administrative und strafrechtliche Verfolgungen und Sanktionen » est remplacée par « verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen » conformément à l'art. 5, let. c, nLPD.

¹⁵² RS 744.103

¹⁵³ RS 745.11

¹⁵⁴ RS 748.132.1

¹⁵⁵ RS 780.11

¹⁵⁶ RS 780.12

¹⁵⁷ RS 784.101.1

Art. 89

Il s'agit d'adapter le renvoi à la nLPD.

7.90 Ordonnance du 6 octobre 1997 sur les ressources d'adressage dans le domaine des télécommunications¹⁵⁸

Art. 13I, al. 2

Il s'agit d'adapter le renvoi à la nLPD.

7.91 Ordonnance du 5 novembre 2014 sur les domaines Internet¹⁵⁹

Art. 17, al. 2, let. f

Il s'agit d'adapter le renvoi à la nLPD.

7.92 Ordonnance du 4 décembre 2000 sur la procréation médicalement assistée¹⁶⁰

Art. 19a, al. 2, 2^e phrase

Il s'agit d'adapter le renvoi à la nLPD.

7.93 Ordonnance du 14 février 2007 sur l'analyse génétique humaine¹⁶¹

Art. 21, al. 3

Il s'agit d'adapter le renvoi à la nLPD.

7.94 Ordonnance du 16 mars 2007 sur la transplantation¹⁶²

Art. 48, al. 3, et 49, 2^e phrase

Il s'agit d'adapter le renvoi à la nLPD et à l'OPDo.

Art. 49c, al. 1, 1^{ère} phrase

Le passage « en sa qualité de maître du fichier » est biffé. Cela n'entraîne aucune modification matérielle.

7.95 Ordonnance du 18 octobre 2017 sur la transplantation croisée¹⁶³

Art. 21, al. 1, 1^{ère} phrase

¹⁵⁸ RS 784.104

¹⁵⁹ RS 784.104.2

¹⁶⁰ RS 810.112.2

¹⁶¹ RS 810.122.1

¹⁶² RS 810.211

¹⁶³ RS 810.212.3

Le passage « en sa qualité de maître du fichier » est biffé. Cela n'entraîne aucune modification matérielle.

7.96 Ordonnance du 16 mars 2007 sur l'attribution d'organes¹⁶⁴

Art. 34c, al. 1, 1^{ère} phrase

Le passage « en sa qualité de maître du fichier » est biffé. Cela n'entraîne aucune modification matérielle.

Art. 34i, al. 1, let a

Le renvoi aux art. 20 et 21 OLPD est remplacé par un renvoi aux art. 1 à 4 et 6 OPDo.

7.97 Ordonnance du 20 septembre 2013 relative à la recherche sur l'être humain¹⁶⁵

Art. 26, al. 2

En allemand, le terme « Datensammlung » est remplacé par « Personendaten ». Par ailleurs, les versions allemande et italienne ont été harmonisées par rapport à la version française par l'ajout de la précision qu'il s'agit de matériel « biologique ».

7.98 Ordonnance d'organisation du 20 septembre 2013 concernant la LRH¹⁶⁶

Art. 11, al. 2, let. a et b

L'art. 11 règle le devoir de l'autorité d'exécution d'informer la personne concernée en cas de communication de données personnelles la concernant. Les exceptions prévues à l'al. 2, let. a et b ne sont pas conformes aux prescriptions de l'art. 20, al. 1, let. a et b nLPD. L'al. 2, let. a doit donc être adapté. Quant à l'exception prévue à l'al. 2, let. b, elle doit être supprimée car elle n'est pas prévue par l'art. 20 nLPD.

Art. 12

Cette disposition règle l'échange de données avec des autorités et des institutions étrangères. Les al. 1, 2 et 3 tiennent compte des nouvelles exigences prévues aux art. 16, al. 1 et 2, let. c et 17, al. 1, let. a et d nLPD.

L'al. 4 reprend l'art. 19, al. 4, nLPD.

¹⁶⁴ RS 810.212.4

¹⁶⁵ RS 810.301

¹⁶⁶ RS 810.308

7.99 Ordonnance du 26 novembre 2008 concernant les examens LPMéd¹⁶⁷

Art. 26, al. 2

La disposition reprend les prescriptions de l'art. 16, al. 1, 1^{ère} phrase et al. 3, OPDo. Elle ne renvoie pas à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès, car contrairement à l'art. 16, al. 1, 2^e phrase, OPDo, la demande ne peut pas être faite oralement en raison du caractère sensible des données personnelles traitées.

7.100 Ordonnance du 14 novembre 2018 sur les autorisations dans le domaine des médicaments¹⁶⁸

Art. 66, let. b

La modification ne concerne que le texte allemand. L'expression « Daten über administrative und strafrechtliche Verfolgungen und Sanktionen » est remplacée par « Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen », conformément à l'art. 5, let. c, ch. 5, nLPD.

Art. 68, al. 2

La première phrase est modifiée de telle façon qu'il ressorte clairement que tous les accès aux systèmes d'information doivent être journalisés. Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.101 Ordonnance du 21 septembre 2018 sur les médicaments¹⁶⁹

Art. 76, al. 2, 2^e phrase

Une adaptation formelle est apportée au texte français afin que la première phrase de l'al. 2 corresponde à la version allemande. Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.102 Ordonnance du 18 août 2004 sur les médicaments vétérinaires¹⁷⁰

Art. 36, titre et al. 5

Dans le titre, le terme de « collections de données » est remplacé par celui de « traitement de données ». Le renvoi à la nLPD est adapté à l'al. 5.

¹⁶⁷ RS 811.113.3

¹⁶⁸ RS 812.212.1

¹⁶⁹ RS 812.212.21

¹⁷⁰ RS 812.212.27

7.103 Ordonnance du 1^{er} juillet 2020 sur les dispositifs médicaux¹⁷¹

Art. 84, al. 1 et 2

Le renvoi à l'OPDo doit être adapté. À l'al. 2, le renvoi aux articles 20 et 21 OLPD est remplacé par les articles 1 à 4 et 6 OPDo.

Art. 92 et annexe 3, 2 Droit suisse, ch. 13, 2^e colonne

Le renvoi à la nLPD doit être adapté.

7.104 Ordonnance du 31 octobre 2018 concernant le système d'information sur les antibiotiques en médecine vétérinaire¹⁷²

Art. 13

Le renvoi à la nLPD de l'al. 1 est adapté. L'al. 2 est adapté afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès.

7.105 Ordonnance du 4 mai 2022 sur les dispositifs médicaux de diagnostic in vitro¹⁷³

Annexe 2, 2 Droit suisse, ch. 7, 2^e colonne

Le renvoi à la nLPD est adapté.

7.106 Ordonnance du 27 février 1991 sur les accidents majeurs¹⁷⁴

Art. 17, titre

Dans le texte allemand, l'expression « Datensammlung » est remplacée par celle de « Datenerhebung ».

7.107 Ordonnance du 20 octobre 2021 sur la restitution, la reprise et l'élimination des appareils électriques et électroniques¹⁷⁵

Art. 8

Il s'agit d'adapter le renvoi à la nLPD.

7.108 Ordonnance du 22 mars 2017 sur le dossier électronique du patient¹⁷⁶

Art. 12, al. 1, 2^e phrase, let. b

Le droit en vigueur prévoit à l'al. 1, let. b que les communautés doivent se doter d'un système de gestion de la protection et de la sécurité des données adapté aux risques et que ce système doit comprendre notamment un inventaire des moyens informatiques et des recueils de données. Cette disposition doit être modifiée en raison de l'introduction par la nLPD

¹⁷¹ RS 812.213

¹⁷² RS 812.214.4

¹⁷³ RS 812.219

¹⁷⁴ RS 814.012

¹⁷⁵ RS 814.620

¹⁷⁶ RS 816.11

(art. 12) d'une nouvelle obligation pour les responsables du traitement d'établir un registre de traitements.

7.109 Ordonnance du 27 mai 2020 sur l'exécution de la législation sur les denrées alimentaires¹⁷⁷

Art. 97, al. 1 à 3

Les al. 1 et 2 de l'art. 97 nécessiteraient d'être modifiés pour respecter la terminologie de la nLPD. Dans la mesure où ils n'apportent rien par rapport à la nouvelle loi et au projet d'ordonnance en matière de protection des données, il est proposé de les abroger.

La modification de l'al. 3 ne concerne que la version allemande. L'expression « Daten über administrative und strafrechtliche Verfolgungen und Sanktionen » est remplacée par « Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen », conformément à l'art. 5, let. c, ch. 5, nLPD.

Art. 98, al. 4

L'expression « pas indispensables » de la deuxième phrase est remplacée par « pas nécessaires » afin que la terminologie de cet alinéa corresponde à celle de l'art. 6, al. 4, nLPD. Seules les données personnelles qui sont nécessaires au destinataire pourront être échangées.

7.110 Ordonnance du 29 avril 2015 sur les épidémies¹⁷⁸

Art. 90, titre

En raison de l'abrogation de la notion de fichier, le titre de l'art. 90 doit être adapté.

Art. 96

Le renvoi aux art. 20 et 21 OLPD est remplacé par un renvoi aux art. 1 à 4 et 6 OPDo.

Art. 97, 2^e phrase

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.111 Ordonnance du 29 avril 2015 sur les laboratoires de microbiologie¹⁷⁹

Art. 23, al. 1, 2^e phrase

Cette modification ne concerne que le texte français. Le terme de « fichier » est remplacé par celui de « dossier ».

¹⁷⁷ RS 817.042

¹⁷⁸ RS 818.101.1

¹⁷⁹ RS 818.101.32

7.112 Ordonnance 1 du 10 mai 2000 relative à la loi sur le travail¹⁸⁰

Préambule, art. 89 et art. 90

Les renvois à la nLPD doivent être adaptés.

7.113 Ordonnance du 19 juin 1995 sur les chauffeurs¹⁸¹

Art. 18 Abs. 6

Les renvois à la nLPD, respectivement à l'OPDo doivent être adaptés.

7.114 Ordonnance du 6 septembre 2006 sur le travail au noir¹⁸²

Art. 9, titre, al. 1, et 9a

En raison de l'abrogation de la protection des données personnelles concernant des personnes morales par la nLPD, le projet de révision de la loi sur le travail au noir introduit à l'art. 17a une nouvelle base légale qui habilite les organes de contrôle cantonaux et les autorités cantonales compétentes à traiter des données concernant des personnes morales (voir annexe 1/II, ch. 78, nLPD). Le projet de révision prévoit de modifier le titre et l'al. 1 de l'art. 9 de l'ordonnance sur le travail au noir en ce sens que cette disposition règle dorénavant uniquement la protection des données personnelles. Il introduit également un nouvel art. 9a qui régit le traitement des données concernant des personnes morales. L'al. 1 de l'art. 9a contient une disposition analogue à l'art. 9 al. 1. L'art. 9, al. 2 à 4, s'applique par analogie aux données des personnes morales, conformément à l'art. 9a, al. 2.

7.115 Ordonnance du 16 janvier 1991 sur le service de l'emploi¹⁸³

Art. 58, titre et al. 1

L'art. 58 de l'ordonnance sur le service de l'emploi règle le droit de la personne concernée à être renseignée par les services qui traitent des données à son sujet.

L'art. 58 doit être adapté pour être conforme aux nouvelles exigences de la nLPD, notamment aux art. 19 nLPD (devoir d'informer lors de la collecte de données personnelles), 25 nLPD (droit d'accès) et 41 nLPD (prétentions et procédure).

La première modification concerne le titre de l'art. 58 qui n'est pas exact. En effet, comme on le verra ci-dessous, cette disposition régit différents droits des personnes concernées, et pas uniquement celui d'être renseigné.

À l'instar du droit en vigueur, l'al. 1 règle le devoir d'informer la personne concernée. Le catalogue des informations à fournir est néanmoins élargi. En vertu du nouvel al. 1, les demandeurs d'emploi et les employeurs qui s'annoncent aux autorités dont relève le marché du travail doivent dorénavant également recevoir des informations sur l'identité et les coordonnées du responsable du traitement (let. a). Les informations prévues aux let. b, c et e restent inchangées, sous réserve de certaines adaptations rédactionnelles. L'information prévue à la let. d est quant à elle modifiée, en ce sens que la personne concernée ne doit plus être

¹⁸⁰ RS 822.111

¹⁸¹ RS 822.221

¹⁸² RS 822.411

¹⁸³ RS 823.111

informée « des destinataires réguliers » mais de tout destinataire ou de toute catégorie de destinataires auxquelles des données sont transmises.

Art. 59a

Cette modification ne concerne que le texte français. Il s'agit de remplacer le terme « fichier » par celui de « registre ».

7.116 Ordonnance du 11 septembre 1996 sur le service civil¹⁸⁴

Art. 110, titre, al. 1 et 2, phrase introductive

Le terme de « fichier » est remplacé par « banques de données ».

7.117 Ordonnance du 20 août 2014 sur le système d'information du service civil¹⁸⁵

Art. 11, al. 1, let. a et 13, al. 1

Il s'agit d'adapter le renvoi à la nouvelle législation sur la protection des données.

Art. 11, al. 4

Cette disposition est mise à jour afin de correspondre aux exigences de journalisation de l'OPDo.

7.118 Ordonnance du 11 septembre 2002 sur la partie générale du droit des assurances sociales¹⁸⁶

Art. 8b, al. 2, 3^e phrase, et 9, al. 2, 2^e phrase

Il s'agit d'adapter le renvoi à la nouvelle législation sur la protection des données.

7.119 Règlement du 31 octobre 1947 sur l'assurance-vieillesse et survivants¹⁸⁷

Art. 144, deuxième phrase

En français, le terme « fichier » est remplacé par « registre ».

7.120 Règlement du 17 janvier 1961 sur l'assurance-invalidité¹⁸⁸

En français, les termes « fichiers de données » sont remplacés par « ensembles de données ».

¹⁸⁴ RS 824.01

¹⁸⁵ RS 824.095

¹⁸⁶ RS 830.11

¹⁸⁷ RS 831.101

¹⁸⁸ RS 831.201

7.121 Ordonnance du 27 juin 1995 sur l'assurance-maladie¹⁸⁹

Art. 30c, 1^{ère} phrase

Il s'agit d'adapter le renvoi à la nouvelle numérotation de l'OPDo.

Art. 59a, al. 1, 3, 1^{ère} phrase, 6, 2^e phrase, 7, 1^{ère} phrase

Les modifications apportées aux al. 1 et 3, 1^{ère} phrase ne concernent que le texte français. Il s'agit de remplacer le terme de « fichier » par celui de « ensemble ». Le texte français est ainsi aligné sur les textes allemand et italien (« Datensatz », respectivement « insieme di dati »)

Les renvois prévus aux al. 6, 2^e phrase et 7, 1^{ère} phrase doivent être adaptés à la numérotation de la nLPD.

Art. 59a, al. 7

Le terme « préposé » est remplacé par « Préposé fédéral à la protection de données et à la transparence » puis par « PFPDT ».

Art. 59a^{ter}, al. 1

Le renvoi aux art. 21 et 22 OLPD est remplacé par un renvoi aux art. 1 à 4 et 6 OPDo car les dispositions relatives à la sécurité des données de la section 1 forment un ensemble. Les dispositions relatives à la sous-traitance continuent de s'appliquer quoi qu'il en soit.

7.122 Ordonnance du 20 décembre 1982 sur l'assurance-accidents¹⁹⁰

Art. 72a, al. 2, 2^e phrase

Il s'agit d'adapter le renvoi à l'OPDo.

7.123 Ordonnance du 31 octobre 2007 sur les allocations familiales¹⁹¹

Art. 18h, al. 1, let. a

Il s'agit d'adapter le renvoi à l'OPDo.

7.124 Ordonnance du 31 août 1983 sur l'assurance-chômage¹⁹²

Art. 126, al. 1

Voir le commentaire de l'art. 58 de l'ordonnance du 16 janvier 1991 sur le service de l'emploi (ch. 7.114).

¹⁸⁹ RS 832.102

¹⁹⁰ RS 832.202

¹⁹¹ RS 836.21

¹⁹² RS 837.02

En outre, le terme de « systèmes d'information » de l'art. 126, al. 1, est utilisé au pluriel, car il en existe plusieurs.

7.125 Ordonnance du 26 mai 2021 sur les systèmes d'information AC¹⁹³

Art. 2, al. 2

Il s'agit d'adapter le renvoi à la nLPD.

7.126 Ordonnance du 18 juin 2021 sur les systèmes d'information consulaires du Département fédéral des affaires étrangères¹⁹⁴

Préambule

En raison des modifications de la LOGA (ch. 13, annexe 1/II nLPD), l'ordonnance se fonde désormais sur l'art. 57^hter LOGA. Le préambule est adapté en conséquence.

Art. 25, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.127 Ordonnance du 28 mai 1997 sur les AOP et les IGP¹⁹⁵

Art. 19, al. 2, let. d, ch. 4, et 21b, al. 2, let. d

Il s'agit d'adapter le renvoi à la nLPD.

7.128 Ordonnance du 22 septembre 1997 sur l'agriculture biologique¹⁹⁶

Art. 33, let. c, ch. 6

Il s'agit d'adapter le renvoi à la nLPD.

7.129 Ordonnance du 25 mai 2011 sur les dénominations «montagne» et «alpage»¹⁹⁷

Art. 11, al. 1, let. d, ch. 4

Il s'agit d'adapter le renvoi à la nLPD.

¹⁹³ RS 837.063.1

¹⁹⁴ SR 852.12

¹⁹⁵ RS 910.12

¹⁹⁶ RS 910.18

¹⁹⁷ RS 910.19

7.130 Ordonnance du 3 novembre 2021 relative à Identitas SA et à la banque de données sur le trafic des animaux¹⁹⁸

Art. 4, titre et al. 4

En français, le terme « fichiers » est remplacé par « ensembles de données ».

7.131 Ordonnance du 27 avril 2022 concernant les systèmes d'information de l'OSAV liés à la chaîne agroalimentaire¹⁹⁹

Art. 25, let. a

Il s'agit d'adapter le renvoi à la nLPD.

7.132 Ordonnance du 18 novembre 2015 réglant les échanges d'importation, de transit et d'exportation d'animaux et de produits animaux avec les pays tiers²⁰⁰

Art. 102d, 2^e phrase

Le terme « règlement d'exploitation » est remplacé par « règlement de traitement »

Art. 102e

Il s'agit d'adapter le renvoi à la nLPD. L'al. 2 est adapté afin de renvoyer à l'art. 16 OPDo en ce qui concerne la forme de la demande d'accès.

7.133 Ordonnance du 26 juin 2013 sur l'obligation des prestataires de services de déclarer leurs qualifications professionnelles dans le cadre des professions réglementées et sur la vérification de ces qualifications²⁰¹

Titre précédant l'art. 9 et art. 9, al. 1

Le titre précédant l'art. 9 a été modifié et s'intitule désormais « traitement des données » au lieu de « collection des données ». La modification relative à l'art. 9, al. 1, ne concerne que l'allemand : « sammelt » a été remplacé par « beschafft ».

7.134 Ordonnance du 24 juin 2015 sur les prestations de sécurité privées fournies à l'étranger²⁰²

Art. 12, al. 1, phrase introductive, 3, phrase introductive et 4

Les modifications apportées aux al. 1 et 3 ne concernent que la version allemande. Conformément à l'art. 5, let. c, ch. 5, nLPD, l'expression « Daten über administrative und strafrechtliche Verfolgungen und Sanktionen » est remplacée par « Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen ». À l'al. 4, le renvoi à la nLPD est adapté.

¹⁹⁸ RS 916.404.1

¹⁹⁹ RS 916.408

²⁰⁰ RS 916.443.10

²⁰¹ RS 935.011

²⁰² RS 935.411

7.135 Ordonnance du 12 août 2015 sur le système de traitement des données relatives aux prestations de sécurité privées²⁰³

Préambule

En raison des modifications de la LOGA (ch. 13, annexe 1/II nLPD), l'ordonnance se fonde désormais sur l'art. 57^hter LOGA. Le préambule est adapté en conséquence.

Art. 9, al. 1, let. a

Il s'agit d'adapter le renvoi à la nLPD.

Art. 10, al. 2

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

7.136 Ordonnance du 7 novembre 2018 sur les jeux d'argent²⁰⁴

Art. 73, al. 3

Il s'agit d'adapter le renvoi à la nLPD.

7.137 Ordonnance du 27 novembre 2000 sur les explosifs²⁰⁵

Titre 9a, art. 117a, 117b, 117f, al. 2, phrase introductive

Il s'agit de remplacer dans la version française les termes « fichier électronique » par celui de « banque de données ».

Art. 117g, 2^e phrase

Conformément à l'art. 4, al. 5, OPDo, les procès-verbaux de journalisation sont conservés séparément du système dans lequel les données personnelles sont traitées.

Art. 117i, 117j, al. 1 et 117k

Il s'agit d'adapter le renvoi à la nLPD. Le terme de « fichier » est supprimé dans la version française de l'art. 117i.

Annexe 14, ch. 13, titre et al. 1

Dans la version française, le terme « fichier » est remplacé par celui de « registre ».

²⁰³ RS 935.412

²⁰⁴ RS 935.511

²⁰⁵ RS 941.411

7.138 Ordonnance du 25 août 2004 sur le Bureau de communication en matière de blanchiment d'argent²⁰⁶

Art. 13, al. 1, let. a

Il s'agit d'adapter la formulation car l'art. 13, al. 2, LOC ne contient plus de conditions mais renvoie à des dispositions du code pénal.

Art. 19, al. 1, let. a, et 26, al. 1, 3^e phrase

Il s'agit d'adapter le renvoi à la nLPD. À l'article 26, al. 1, 3^e phrase, le terme « Office fédéral des migrations » est remplacé par « Secrétariat d'État aux migrations ».

Art. 25, al. 1, 1^{ère} phrase

Le terme d'« exhaustivité » est ajouté à cette disposition afin qu'elle corresponde à l'art. 29 OPDo.