Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la justice OFJ
Domaine de direction Droit public

31 août 2022

Révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD)

Rapport sur les résultats de la procédure de consultation

BJ-D-BF633401/238

Table des matières

1 Contexte

Le 25 septembre 2020, le Parlement a adopté la révision totale de la loi sur la protection des données. Cette révision a pour but non seulement d'adapter le droit suisse de la protection des données à l'ère du numérique, mais également de garantir un niveau de protection reconnu sur le plan international.

L'ordonnance relative à la loi sur la protection des données (OLPD) contient les dispositions générales d'exécution de la loi sur la protection des données ainsi que certaines dispositions de substitution. Cela signifie qu'elle vise principalement à préciser la loi sur la protection des données à l'aide de dispositions plus détaillées et à faciliter son application. Ainsi elle s'applique aussi bien aux traitements de données effectués par des personnes privées (en particulier des entreprises) qu'à ceux effectués par des organes fédéraux. En revanche, s'agissant des traitements de données réalisés par des organes cantonaux ou communaux, c'est en principe le droit cantonal sur la protection des données qui est applicable.

2 Procédure de consultation

Le 23 juin 2021, le Conseil fédéral a ouvert la procédure de consultation relative au projet d'ordonnance. Elle a pris fin le 14 octobre 2021. Ont été invités à participer les cantons, les partis politiques représentés à l'Assemblée fédérale, les associations faîtières de l'économie, des communes, des villes et des régions de montagne qui œuvrent au niveau national ainsi que d'autres organisations concernées. Au total, 123 prises de position ont été reçues. Ont notamment pris position 24 cantons[1], la Conférence des préposés cantonaux à la protection des données « privatim », six partis politiques[2] ainsi que de nombreuses associations issues des milieux proches de l'économie, de la protection des consommateurs et de la protection des données[3].

Deux cantons (NE, TI), le Tribunal fédéral ainsi que le Tribunal pénal fédéral ont expressément renoncé à prendre position. Si le canton d'Obwald n'a pas pris position, il a toutefois transmis l'avis de son autorité cantonale en matière de protection des données. De même, l'Union patronale suisse n'a pas pris position. Le projet a été traité par economiesuisse conformément à une répartition des dossiers entre les deux associations.

[1] Cantons : AG, AI, AR, BE, BL, BS, FR, GE, GL, GR, LU, NE, NW, OW, SG, SH, SO, SZ, TG, TI, UR, VD, VS, ZH. Manquent : JU, ZG.

[2] Partis : Le Centre, PLR, PPS, PS, PVS, UDC.

[3] Exemple d'organisations : DigiGes, economiesuisse, Stiftung für Konsumentenschutz, SwissHoldings, usam.

3 Résultats de la procédure de consultation

3.1 Remarques générales

10 cantons[4], 2 partis[5] et 6 organisations[6] adhèrent au projet sur le fond, même si la plupart estiment qu'il existe encore du potentiel d'amélioration. À cet égard, de nombreux cantons se réfèrent à privatim.

2 cantons[7], 2 partis[8] et 29 organisations[9] rejettent nettement le projet, ou s'expriment de manière très critique à son égard.

D'autres participants à la procédure de consultation (5 cantons[10], un parti[11] et 44 organisations[12]) émettent des doutes ou sont très critiques.

4 cantons[13], le Tribunal administratif fédéral et 11 organisations ou personnes privées[14] commentent le projet et formulent des propositions d'amélioration, sans prendre position pour ou contre le projet.

3.1.1 Points essentiels

L'opinion qui ressort de nombreuses prises de position est celle selon laquelle plusieurs normes[15] sont dépourvues de base légale[16], ou qu'il n'a pas été tenu compte de la volonté du législateur dans la mesure où certaines règles ont été formulées à l'encontre de la teneur des délibérations parlementaires[17]. Certains participants sont d'avis que le projet d'ordonnance est en partie contraire à la nLPD[18]. Dans ce sens, certains émettent le souhait que les dispositions de l'ordonnance se réfèrent clairement aux normes légales concernées[19]. De plus, il

4 Cantons : AI, BE, BS, GL, LU, NW, SG, TG, VS, ZH.

5 Partis : Le Centre, PS.

6 Organisations : DFS, FER, FMH, UPSV, USS, UVS.

7 Cantons : UR, VD.

8 Partis : PLR, UDC.

9 Organisations : AFBS, ASA, Association de commerce, CFF, Coop, digitalswitzerland, economiesuisse, GastroSuisse, H+, HKBB, Hotellerie Suisse, la Poste, les banques domestiques, Migros, pharmaSuisse, Raiffeisen, rega, Ringier, SBV, Scienceindustries suisse, SDV, suva, thurbo, UBCS, usam, UTP, veb.ch, VUD, Walderwyss.

10 Cantons : AG, AR, GR, SH, SZ.

11 Parti : PVS.

12 Organisations : ADIDE, ASIP, ASP, ASPS, ASSL, Association de commerceIGEM, asut, ATPrD, auto suisse, BNS, Bär & Karrer, CFC, CP, Creditreform, curafutura, CURAVIVA, datenschutzguide.ch, EPS, EXPERTsuisse, Forum PME, FRC, FSA, FSEP, INSOS, IS, Privacy Icons, privatim, proFonds, santésuisse, senesuisse, SPA, Spitex suisse, SSMD, Stiftung Konsumentenschutz, suisa, Sunrise UPC, SWICO, Swiss Insights, SwissFoundations, SwissHoldings, swissICT, swissstaffing, UPSA, vsi.

13 Cantons : BL, FR, GE, SO.

14 Organisations : ASDPO, Bibliosuisse, Classtime, CYBER SAFE, DigiGes, ETH Bibliothek, HÄRTING, HDC, Swimag, swissprivacy.law ; personne privée : Beat Lehmann.

15 art. 1, al. 2, art. 3, art. 4, art. 5, art. 6, al. 2, art. 9, al. 1, let. j et k, art. 15, art. 16, art. 17, art. 18, art. 19, al. 1, let. b à d, al. 2, al. 3 et al. 5, art. 20, al. 5, art. 31 et art. 32 P-OLPD.

16 Cantons : BE, SZ, UR, VD (concernant le traitement de données sensibles) ; organisations : ASB, ASSL, asut, BNS, Bär & Karrer, Coop, Creditreform, Datenschutzguide.ch, economiesuisse, EXPERTsuisse, Forum PME, FSA, GastroSuisse, H+, HKBB, HotellerieSuisse, IGEM, la Poste, les banques domestiques, Migros, pharmaSuisse, Raiffeisen, rega, Ringier, SSMD, suisa, Sunrise UPC, suva, SWICO, Swiss Insights, SwissFoundations, SwissHoldings, swissICT, swissstaffing, UBCS, UPSA, usam, UTP, veb.ch, vsi, VUD, Walderwyss ; parti : UDC.

17 Organisations : Association de commerce, auto suisse, Coop, Creditreform, digtialswitzerland, economiesuisse, EXPERTsuisse, Forum PME, FSA, H+, HKBB, HotellerieSuisse, IGEM, les banques domestiques, Raiffeisen, rega, Ringier, Scienceindustries suisse, suisa, suva, SWICO, Swiss Insights, SwissHoldings, UPSA, veb.ch, vsi, VUD ; parti : UDC.

18 Organisations : ASSL, auto suisse, digitalswitzerland, EXPERTsuisse, Raiffeisen, Swiss Insights.

19 Organisations : ASP, Creditreform, DFS, EPS, FSA, FSEP, IGEM, swissstaffing, vsi.

est reproché à l'ordonnance de ne pas refléter suffisamment l'orientation de base suivie par la nLPD, à savoir l'approche fondée sur le risque[20] [21].

Certains participants sont d'un avis contraire et estiment que le P-OLPD respecte le cadre de la nouvelle loi sur la protection des données (nLPD), voire le restreint à certains égards[22]. C'est pourquoi certains estiment qu'il est primordial que le Conseil fédéral continue à utiliser résolument sa marge de manœuvre pour davantage de protection des données et évite de vider l'art. 61, let. c, nLPD de sa substance en adoptant des mesures incomplètes ou peu claires[23].

Le souhait est que les points supplémentaires soient réglés, par exemple l'analyse d'impact relative à la protection des données personnelles, la remise et la portabilité des données personnelles)[24].

Selon une critique récurrente sur l'ensemble du projet, les dispositions de l'ordonnance manquent de précision et laissent une marge d'interprétation trop importante ou génèrent un manque de clarté[25]. Il est également reproché au projet d'utiliser une terminologie obsolète. Il reprend de nombreuses dispositions dépassées issues de l'actuelle OLPD[26]. Certains participants sont d'avis que de nombreuses dispositions sont incompatibles avec les bases légales figurant dans la nLPD[27]. Des termes imprécis ou vagues ont été repris tels quels de différentes sources[28]. Il en résulte un projet global peu intelligible et dénué de cohérence terminologique[29]. Plusieurs participants souhaitent que les explications du rapport figurent dans le texte même de l'ordonnance[30].

Certains participants reprochent, au contraire, aux dispositions du projet d'être trop détaillées et trop étendues, et par conséquent d'occasionner une charge de travail disproportionnée, voire des conséquences négatives imprévues[31]. En particulier, certains soulignent le risque de chevauchement entre l'objectif et le contenu de l'analyse d'impact relative à la protection

[20] Par « approche fondée sur le risque », on entend que les obligations du responsable du traitement doivent toujours être définies en tenant compte de de la nature, de l'étendue, des circonstances et de la finalité du traitement ainsi que la probabilité et le degré de risque que le traitement présente pour la personnalité et les droits fondamentaux des personnes physiques concernées.

[21] Canton: BL; organisations : ASB, la Poste, privatim, UBCS. Le canton de VD estime par contre que cette approche a été mise en oeuvre de manière rigoureuse, en particulier dans les dispositions relatives à la sécurité des données.

[22] Organisation : DigiGes.

[23] Parti : PS; organisations : FRC, USS.

[24] P. ex. partis: PS, PVS; organisations: DigiGes, FRC, Stiftung für Konsumentenschutz, USS.

[25] Cantons: AG, AR, GL, GR, NW, SH, VD ; organisations : Association de commerce, ATPrD, CYBER SAFE, digitalswitzerland, economiesuisse, FRC (concernant le profilage à risque élevé et la protection des données par le biais de mesures techniques et de préréglages appropriés), HKBB, pharmaSuisse, Préposé à la protection des données de SZ, OW et NW, privatim, Raiffeisen, Scienceindustries suisse, Stiftung für Konsumentenschutz, veb.ch.

[26] Cantons : GR, SH, VD; organisations : privatim, Ringier.

[27] Organisations : DFS, FMH, FSA, H+, HKBB, Migros.

[28] Organisations : Association de commerce, BNS, CFC, CP, CURAVIVA, DFS, FMH, H+, INSOS, la Poste, santésuisse, senesuisse, Stiftung für Konsumentenschutz.

[29] Organisations : DFS, FMH, FSA, H+, HKBB, Migros.

[30] Organisations : ATPrD, DFS.

[31] Cantons : SZ, ZH ; organisations : Coop, digitalswitzerland, economiesuisse, FMH, H+, IGEM, la Poste, proFonds, SWICO, UBCS, VUD, Walderwyss.

des données personnelles, le règlement de traitement, les registres des activités de traitement et l'obligation de journalisation[32]. De manière générale, les participants déplorent la présence de doublons[33]. Les exigences en partie très restrictives sont, selon certains participants, (en particulier pour les PME) inapplicables en pratique[34]. Le canton de Fribourg est favorable aux dispositions ouvertes figurant dans le projet[35].

Divers participants regrettent que l'ordonnance présente de nombreuses spécificités suisses qui ne sont pas prévues comme telles dans la loi et vont même au-delà des exigences du RGPD (« Swiss Finishes »[36])[37]. De nombreux participants estiment que ces dispositions créent souvent une charge de travail excessive pour l'économie privée et pourraient ainsi entraîner un désavantage concurrentiel pour les entreprises suisses[38].

Indépendamment de ce qui précède, le régime transitoire de la nLPD, considéré comme lacunaire, est également critiqué. En particulier, de nombreux participants préconisent l'introduction de délais transitoires adaptés pour l'ensemble des éventuelles nouvelles obligations introduites dans l'ordonnance[39]. Il convient toutefois de veiller à ce qu'une décision d'adéquation soit rendue par la Commission européenne[40]. Parmi les remarques positives, certains participants saluent l'harmonisation avec le droit européen[41].

Deux participants apprécient l'amélioration de la structure et de la systématique, ainsi que le langage plus clair[42]. Un autre point qui est bien accueilli est celui de la concrétisation du droit d'accès[43]. Le CP fait remarquer que les nouvelles règles constituent une condition pour que la numérisation et l'innovation, dont l'importance est vouée à augmenter de manière exponentielle au cours des prochaines années, soient acceptées par la société. Elles représentent ainsi un facteur essentiel du progrès économique suisse[44], de même qu'une occasion pour les entreprises d'optimiser leurs processus[45].

[32] P. ex. organisation : SWICO.

[33] Organisations: auto suisse, BNS, santésuisse.

[34] Parti : UDC ; organisations : Association de commerce, Bär & Karrer, digitalswitzerland, FSA, H+, HKBB, Scienceindustries suisse, SwissFoundations, thurbo, Walderwyss.

[35] Et organisation: CP.

[36] Un « Swiss Finish » est une règlementation suisse qui va plus loin que l'exige la législation européenne, dans notre contexte, le RGPD, sans générer un avantage pour les acteurs suisses opérant sur le marché européen. Au contraire, les « Swiss Finishes » sont la plupart du temps considérés comme étant des freins à la compétitivité des entreprises suisses.

[37] Organisations : ASB, ASP, ASSL, Association de commerce, asut, auto suisse, Creditreform, economiesuisse, EPS, EXPERTsuisse, Forum PME, FSA, FSEP, HKBB, la Poste, Migros, Raiffeisen, Ringier, Scienceindustries suisse, Sunrise UPC, Swiss Insights, SwissHoldings, swissstaffing, UBCS, UPSA, usam, vsi.

[38] Organisations : Asut, digitalswitzerland, EXPERTsuisse, FER, Forum PME, FSA, HKBB, la Poste, Migros, Ringier, Scienceindustries suisse, Sunrise UPC, SWICO, SwissHoldings, UBCS.

[39] Organisations : ASA, ASIP, Coop, curafutura, FSA, la Poste, IGEM, pharmaSuisse, Raiffeisen, rega, usam, swissstaffing, VUD, Walderwyss.

[40] Organisations : ASA, ASIP, Coop, curafutura, FSA, IGEM, la Poste, pharmaSuisse, Raiffeisen, rega, swissstaffing, usam, VUD, Walderwyss.

[41] Organisations: ASSL, BNS, Digitalswitzerland, H+, UVS.

[42] Canton : VS et organisation : DFS.

[43] Parti: Le Centre; organisation: Stiftung für Konsumentenschutz.

[44] Et organisations : GastroSuisse, UPSV.

[45] Organisations : CP, UPSV.

3.1.2 Remarques générales

3.1.2.1 Sécurité des données

L'ensemble de la section (art. 1 à 5) fait l'objet de nombreuses critiques. Elle est considérée comme imprécise et insuffisamment détaillée. La crainte est que l'utilisation de notions juridiques indéterminées n'affaiblisse l'étendue de la protection ainsi que la possibilité de recourir aux dispositions pénales. Il est également reproché aux dispositions d'être trop détaillées. Dans certains cas, la structure, de même que les choix terminologiques, sont remis en question. L'absence de base légale est, en outre, fréquemment soulevée.

La section a également reçu des commentaires positifs. L'approche fondée sur les risques est soutenue par un grand nombre de participants[46]. La structure choisie est accueillie favorablement par certains participants[47], notamment la différence opérée selon le type et les activités de l'entreprise. Bär & Karrer comprend, en outre, la réticence du Conseil fédéral d'introduire dans l'ordonnance des exigences spécifiques minimales et salue le renforcement de la sécurité des données. Des cantons[48] saluent la formulation ouverte des dispositions qui permet une large mise en oeuvre. LU est, toutefois, d'avis que le prononcé d'une amende sur la base de la violation de ces dispositions est peu adapté. À la lumière du principe de la sécurité du droit, il demande qu'une clarification soit apportée concernant le lien entre les dispositions de cette première section et l'art. 61 nLPD. Selon UPSV, une formulation générale a des avantages. Il s'interroge, néanmoins, sur la latitude d'interprétation laissée à la jurisprudence. Cette délégation au pouvoir judiciaire constitue une possible violation du principe de la séparation des pouvoirs. Il propose une terminologie plus distinctive. H+ accueille avec satisfaction l'élaboration d'exigences minimales peu rigides ; rappelant qu'il serait délicat de fixer des exigences générales valables pour toutes les branches. VS soutient les exigences minimales à respecter s'agissant de la sécurité des données. Il comprend que ces « lignes directrices » soient envisagées de manière souple.

Sur les considérations générales, un grand nombre de participants[49] sont d'avis que le projet ne concrétise pas les exigences minimales (art. 8 nLPD). Le principe de la légalité en droit pénal exige qu'un acte soit expressément réprimé par la loi pour être punissable (art. 8, al. 3, et art. 61, al. 1, let. c, nLPD). Pourtant, le projet ne permet pas de définir avec suffisamment de précision l'absence de quelle mesure réaliserait une infraction pénale. Ainsi les mesures minimales doivent être détaillées. H+ rejette les dispositions de cette section, qui, selon lui, ne reposeraient sur aucune base légale. Trop détaillées, ne prenant pas en compte la diversité des activités de traitement et des situations avec le risque d'engendrer une surcharge administrative, elles contrediraient la volonté du législateur. D'autres participants[50] se sont exprimés dans le même sens. Ils déplorent, en outre, la reprise des concepts de l'OLPD actuelle simplement complétés de principes issus du droit européen[51]. Ils invitent le Conseil fédéral à

[46] Cantons : AG, BE, BL, GL, LU, NW, OW, SO, SZ, ZH ; organisations : ASA, ASP, ASSL, ATPrD, CFF, Creditreform, curafutura, Datenschutzguide.ch, digitalswitzerland, economiesuisse, H+, HKBB, la Poste, les banques domestiques, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim, Raiffeisen, Scienceindustries suisse, SDV, SPA, suva, swissICT, thurbo, UTP, vsi. L'approche fondée sur le risque appelle toutefois quelques ajustements.

[47] Organisations : ATPrD, Bär & Karrer.

[48] Cantons : FR, LU.

[49] Cantons : AI ; parti politique : PVS ; organisations : ASDPO, FRC, HDC, Swissprivacy, UBCS, veb.ch. D'autres participants partagent cette opinion tout particulièrement concernant l'art. 2. À ce sujet, voir nbp n. 98.

[50] Cantons : AG, AR, BE, GL, GR, NW, SH, SZ, VD, ZU, PVS. VD soutient la demande de révision et insiste particulièrement sur l'art. 1, al. 1 ; parti politique : PVS ; organisations et personnes privées : ATPrD, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim, Ringier ; personne privée : Beat Lehmann.

[51] À ce sujet, voir nbp n. 97.

réviser toute la section et, à cet effet, ils citent, à titre d'exemple, la loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération[52]. Des participants[53] proposent également de s'inspirer de l'art. 32, al. 1 RGPD, voire de préciser les mesures.

VD propose d'inclure dans cette première section des critères indiquant la pertinence, voire l'obligation, de conduire des analyses d'impact relative à la protection des données (AIPD) afin de concrétiser et développer la notion de « risque accru pour la personnalité et les droits fondamentaux de la personne concernée » de l'art. 16 al. 1 nLPD.

Des participants[54] demandent de ne pas vider ces dispositions de leur sens avec des mesures trop modestes, voire peu explicites. Ils regrettent, en outre, l'utilisation de notions juridiques indéterminées[55].

3.1.2.2 Communication de données personnelles à l'étranger

GL salue l'ensemble des dispositions de la section (art. 8 à 12), qui pourront servir d'inspiration au droit cantonal. Quelques participants[56] rappellent l'importance de ces dispositions et jugent les exigences pertinentes.

3.2 Avis sur les différents articles

3.2.1 Art. 1 P-OLPD : Principes

Les principes introduits dans ce premier article sont salués par deux participants[57].

Al. 1

Plusieurs participants[58] saluent la formulation proposée par cette disposition, qui concrétiserait de manière optimale l'art. 8, al. 1, nLPD. Ce nonobstant, la latitude d'interprétation demande un soutien ponctuel dans la pratique. Ils suggèrent d'ajouter, notamment dans un nouvel alinéa, que le « PFPDT doit créer dans les plus brefs délais des documents simplifiant la mise en œuvre pratique ». D'un avis contraire, le DFS estime que la formulation ne fait pas honneur à l'art. 8, al. 1, nLPD. Il propose d'ajouter l'art. 8, al. 1, nLPD comme phrase introductive à l'art. 1. Concernant les critères, il se justifierait de mentionner « notamment ». La FMH propose d'ajouter en introduction « des mesures techniques et organisationnelles appropriées doivent être prises pour assurer un niveau de sécurité approprié selon le risque ». L'ASDPO demande de préciser que les mesures minimales peuvent être sélectionnées dans la liste de l'art. 2. Classtime souhaite ajouter « l'utilité du traitement » à l'art. 1.

Selon quelques participants[59], l'uniformité terminologique doit être garantie. Ainsi les mesures ne sont pas « adaptées », mais « appropriées » conformément à l'art. 8, al. 1, nLPD. En outre, ils sont d'avis que la concrétisation de l'art. 8 nLPD va au-delà de la sécurité des

[52] LSI, RO **2020** 232.

[53] Cantons : AG, AR, BE, GL, NW, SH, SZ, VD, ZH ; organisations : ATPrD, Bär & Karrer, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim. À ce sujet, voir nbp n. 60.

[54] Organisations : DigiGes, FRC, Stiftung für Konsumentenschutz.

[55] À ce sujet, voir les commentaires sous l'art. 1, al. 2, et l'art. 2, phrase introductive.

[56] Parti politique : PS ; organisation : USS.

[57] Organisations : ASDPO, FER.

[58] Canton : VD ; organisations : Aide et soins à domicile Suisse, ASPS, CURAVIVA.CH, INSOS, IS, senesuisse. Forum PME soutient ce besoin de soutien du PFPDT, mais avec une vision plus critique du projet. Le CP propose la même approche, notamment pour les nouvelles définitions ajoutées dans la nLPD, dont le « profilage à haut risque ».

[59] Organisations : CFF, FSA, H+, IGEM, la Poste, Migros, Ringier, suva, thurbo, UTP, VUD, Walderwyss.

données au sens étroit (CAID : Confidentialité, Authenticité, Intégrité, Disponibilité). Dans cet ordre d'idées, ils jugent les exemples cités incorrects et la portée du terme « risque » erronée. Il s'agit du risque net et non du risque brut. Ainsi le traitement par l'intelligence artificielle (IA) ou l'être humain n'est pas pertinent pour la question de la sécurité des données.

De manière générale, un grand nombre de participants[60] relèvent l'influence du droit européen, et notamment de l'art. 32 RGPD. Ils proposent de s'en inspirer ainsi que de la LSI. Ils sont d'avis que l'approche doit se faire en deux étapes : évaluer premièrement les objectifs de protection, les besoins de protection et les risques. Quoique les objectifs de protection soient énoncés à l'art. 5, al. 1, let. h, nLPD et détaillés à l'art. 2, la distinction opérée par cet alinéa entre critères à même de permettre l'évaluation du besoin de protection (let. a), l'évaluation du risque (let. b) et l'adéquation des mesures est jugée bienvenue. Toutefois, comme pour l'analyse d'impact sur la protection des données, l'évaluation du risque intervient dans un second temps (art. 22 nLPD). Concernant les critères relatifs à l'adéquation des mesures, ils regrettent leur caractère indirect. L'opportunité d'une mesure doit permettre d'évaluer si une mesure doit être prise et, concrètement, laquelle permet de contrer le risque avec l'efficacité nécessaire. Deux cantons[61] considèrent également « l'état de la technique » comme un critère indirect. SZ se demande si les critères d'adéquation sont cumulatifs. Ce qu'il trouverait regrettable. ZH s'oppose également à cet aspect cumulatif. Il souligne que les objectifs de protection (art. 5, let. h, nLPD), le besoin de protection (art. 1, al. 1, let. a) et les risques (art. 22 nLPD) devraient ressortir plus clairement de la disposition.

BL propose d'harmoniser la méthodologie à l'image de la Confédération avec HERMES. L'art. 1 devrait ainsi refléter l'évaluation des risques et les mesures à prendre en fonction de l'état actuel des connaissances techniques.

Le PS estime que le risque de violation de la sécurité des données est un critère d'évaluation plus pertinent pour les mesures à prendre.

Al. 1 let. a

VD propose d'insérer à la let. a « des critères de profilage, de transferts internationaux et de sous-traitance (Cloud) ».

Eu égard au contenu, SPA conteste le lien entre les critères cités et le risque que présente un traitement de données. Il propose de mentionner expressément les critères au moyen desquels un risque peut être établi conformément à l'art. 8, al. 1, nLPD. Un autre participant[62] demande la suppression du terme « circonstances », le jugeant compris dans celui de « nature » du traitement de données. Il propose de prendre en considération le projet de la Commission européenne relatif au Règlement sur l'intelligence artificielle.

Al. 1 let. b

Divers participants[63] sont d'avis que les coûts de mise en œuvre doivent être pris en compte selon l'art. 1, al. 1, let. b ; c'est-à-dire lors de l'appréciation de l'opportunité d'une mesure, et

[60] Cantons : AG, AR, BE, GL, NW, SH, SZ, VD, ZH ; organisations : ATPrD, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim.

[61] Cantons : NW, SZ.

[62] Organisation : DFS.

[63] Organisations : ASSL, auto suisse, SwissInsights, UPSA.

pas seulement lorsqu'il est décidé quelle mesure est appropriée. Des participants[64] proposent d'ajouter que la probabilité n'a de sens qu'en présence d'un risque. Ce dernier découle d'une violation potentielle de la sécurité des données, et non inversement. Dans cet ordre d'idées, le texte devrait être le suivant : « les effets potentiels subséquents d'une violation de la sécurité des données pour les personnes concernées et leur probabilité ».

La probabilité est un calcul mathématique[65]. Ainsi la classification proposée ne peut être suivie (faible, moyenne ou élevée). À tout le moins, la « probabilité » devrait être remplacée par les « conséquences », voire des critères mathématiques devraient être introduits.

Certains participants[66] demandent que le risque résiduel soit pris en compte.

Al. 1 let. c

L'état de la technique doit être « éprouvé ». Dans cet ordre d'idées, il sied d'ajouter l'« état de la science » comme critère, celui-ci étant depuis des années universellement reconnu[67]. HÄRTING appelle à quelques précisions autour de l'expression « l'état de la technique », notamment en lien avec les sanctions pénales de l'art. 61, let. c, nLPD et propose de remplacer celle-ci par « les règles générales de la technique ».

Al. 1 let. d

Plusieurs participants[68] critiquent la prise en compte des coûts et proposent soit de biffer la let. d, soit de remanier cette disposition. Le besoin de précision est maintes fois invoqué, par exemple pour les « coûts de mise en œuvre », que ce soit pour les PME, les fondations, les associations de petite à moyenne importance ou encore les start-up (concernant le plafond de coûts entre le chiffre d'affaires (projeté) et les coûts de mise en œuvre). Tout en déclarant que ce critère ne concerne que le choix de la variante la plus rentable – parmi celles efficaces –, il est souligné qu'il n'est ni un passe-droit ni une dérogation à l'obligation de garantir la sécurité des données. Au contraire, ce critère doit permettre de réaliser ces exigences, notamment pour les petites et moyennes structures[69]. Des participants[70] considèrent également que les « coûts de mise en œuvre » impliquent, à tort, que les autres dépenses ne sont pas pertinentes. Le rapport explicatif ne devrait pas affirmer que les coûts excessifs ne sont pas utiles.

Un grand nombre de participants[71] proposent de remplacer « coûts de mise en œuvre » par « effort de mise en œuvre », estimant la première expression trop étroite. BE déclare que d'autres critères de mise en œuvre peuvent être pertinents (dépenses élevées en termes de personnel ou en termes de temps et d'organisation). Le rapport explicatif gagnerait à plus de précision. D'autres participants[72] partagent cet avis et regrettent que les explications concernant la prise en compte des coûts de mise en œuvre comme critère dans l'évaluation de

64 Organisations : ASB, digitalswitzerland, economiesuisse, HKBB, la Poste, les banques domestiques, Raiffeisen, Scienceindustries suisse, SDV, swissICT.

65 Organisation : Association de commerce.

66 Organisations : HÄRTING, suva, swissICT.

67 Organisation : Swimag.

68 Partis politiques : PVS, PS ; organisation : USS.

69 Organisations : Association de commerce, Hotelleriesuisse, PES, proFonds, UPSV.

70 Organisations : Association de commerce, CFF, Creditreform, H+, la Poste, Migros, proFonds, Ringier, SPA, suva, thurbo, UTP, VUD, Walderwyss.

71 Canton : BE ; organisations : ASB, ASSL, Bär & Karrer, FMH, la Poste, Raiffeisen, Ringier, santésuisse, suva, swissICT, swissstaffing, UPSA, usam, vsi, VUD.

72 Organisations : ASSL, PES, SPA, UPSA.

l'adéquation soient imprécises. ProFonds indique, à ce propos, que le caractère approprié de la mesure doit être évalué non seulement en fonction des coûts de mise en œuvre, mais également à la lumière de tous les autres coûts. Certains participants[73] ajoutent l'effort général de mise en œuvre. Pour quelques participants[74], les autres dépenses doivent être prises en compte en vertu du principe de la proportionnalité. Il n'est, dès lors, pas nécessaire de les mentionner explicitement.

Divers participants[75] accueillent avec satisfaction le « coût de mise en œuvre » comme critère d'adéquation, jugeant bienvenu que l'effort pour les responsables soit clairement inclus. Il propose, toutefois, de le remplacer par « dépenses pour les responsables ».

Deux participants[76] font remarquer qu'il est peu judicieux de mentionner expressément les coûts de mise en œuvre comme critère d'évaluation de l'opportunité de telles mesures dans l'ordonnance. Le risque de violation de la sécurité des données est le critère d'évaluation pertinent pour les mesures à prendre. Swimag souhaite, au contraire, une formulation précise comprenant l'ajout des moyens minimaux à mettre en place, l'effort ainsi que les coûts.

Al. 2

La suppression de cet alinéa est demandée[77]. À tout le moins, bon nombre de participants[78] demandent de remplacer « intervalles appropriés » par de « manière appropriée ». Selon SZ, ces « intervalles appropriés » ne sont pas très efficaces. Il estime plus pertinent d'opter pour des « mesures réexaminées de manière globale ». D'autres participants[79] trouvent également que l'expression « intervalle approprié » est sujette à interprétation et proposent de la remplacer par « intervalle périodique ». Quelques participants[80] appellent à plus de clarté et insistent sur un réexamen « au moins une fois par an ». La Stiftung für Konsumentenschutz propose un « intervalle périodique et approprié ». Certains[81] demandent que les mesures soient réexaminées « en cas de modifications tangibles des risques ». L'Association de commerce précise que les mesures ne doivent être réexaminées que si les conditions de l'art. 1, al. 1, let. a à c, changent. D'autres participants[82] sont d'avis que le responsable est seul à même d'évaluer l'opportunité du réexamen, et ce tout au long du traitement. Quelques participants[83] contestent le lien entre l'art. 8, al. 3, nLPD et cette exigence supplémentaire d'« examen à intervalles appropriés ». Selon des participants[84], l'examen doit avoir lieu en permanence. La FRC déclare, à ce propos, que la fréquence doit être exempte d'interprétation.

---

73 Organisations : ASSL, auto suisse, FSA, SwissInsights, UPSA.

74 Organisations : ASB, digitalswitzerland, economiesuisse, HKBB, la Poste, les banques domestiques, Raiffeisen, SDV, Scienceindustries suisse, swissICT.

75 Organisations : ASP, Creditreform, EPS, FSEP, vsi.

76 Parti politique : PS ; organisation : USS.

77 Organisation : SPA.

78 Organisations : ASSL, ASB, auto suisse, CFF, digitalswitzerland, economiesuisse, FSA, H+, HKBB, IGEM, la Poste, les banques domestiques, Migros, Raiffeisen, Ringier, santésuisse, Scienceindustries suisse, SDV, SPA, SSMD, suva, SwissInsights, swissstaffing, thurbo, UPSA, UTP, VUD, Walderwyss.

79 Organisations : santésuisse, UPSV.

80 Organisations : Aide et soins à domicile Suisse, ASPS, CURAVIVA.CH, INSOS, IS, senesuisse.

81 Organisations : ASP, Creditreform, EPS, FSEP, usam, vsi.

82 Organisations : SwissICT, Walderwyss.

83 Organisations : ASP, Creditreform, EPS, FSEP, vsi.

84 Cantons : AG, BE, GL, NW, VD ; organisations : ATPrD, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim.

Sous l'angle terminologique, « l'évaluation des risques » est préférée à « mesures »[85]. Certains participants[86] font remarquer que l'examen porte sur les facteurs de risque. BE propose de préciser que « les risques et les mesures sont réexaminés ».

EXPERTsuisse recommande de standardiser le contrôle en rendant obligatoire la norme ISO 27001.

Finalement, il convient de s'aligner aux droits européen et international et d'opérer une distinction pour les données archivées[87].

3.2.2 Art. 2 P-OLPD : Objectifs de protection

La disposition a reçu quelques retours positifs parmi les prises de position. Certains participants[88] accueillent la liste d'objectifs avec satisfaction, la qualifiant d'aide-mémoire. Ils font néanmoins remarquer le besoin d'un soutien ponctuel par les autorités compétentes, notamment par le PFPDT. Ils proposent d'introduire dans le texte légal qu'un accès au PFPDT, à des coûts raisonnables, est offert aux entreprises suisses ; à tout le moins, ce catalogue (aide-mémoire) devrait faire l'objet d'une annexe[89].

Quelques participants[90] pensent que les exigences énumérées à l'art. 2 sont celles visant à garantir les objectifs de protection. Ainsi il se justifie de s'inspirer de l'art. 6, al. 2, LSI et modifier la phrase introductive. Les objectifs de protection étant des cibles, les mesures doivent être appropriées par rapport aux risques identifiés dans l'évaluation des risques. Des participants[91] proposent, à titre d'exemple, de s'inspirer de la loi sur l'information et la protection des données des cantons de BS et ZH.

La disposition est, tout de même, largement critiquée. Pour un grand nombre de participants[92], une révision est indispensable. Quoique l'influence de l'art. 5, al. 1, let. h, nLPD ou encore de l'art. 32, ch. 1, RGPD soit appréciée, les objectifs cités doivent se limiter à la confidentialité, l'intégrité, la disponibilité et la traçabilité. La volonté est de formuler des exigences minimales et non des exigences maximales. S'aligner au droit européen facilitera la mise en œuvre de la nLPD et du RGPD[93]. Dans cet ordre d'idées, des participants[94] exigent la suppression de tout Swiss Finish. Il découle de la disposition une obligation de documentation

85 Cantons : BE, GL ; organisations : ATPrD, FMH, privatim.

86 Canton : BE ; organisation : DigiGes.

87 Personne privée : Beat Lehmann.

88 Organisations : Aide et soins à domicile Suisse, ASPS, CURAVIVA.CH, INSOS, IS, senesuisse.

89 Personne privée : Beat Lehmann.

90 Cantons : AG, BE, GL, SH, VD, ZH ; organisations : ATPrD, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim.

91 Cantons : AR, NW, SZ ; organisation : Préposé à la protection des données de SZ, OW et NW.

92 Cantons : AG, BE, AR, GL, NW, SZ, TG, VD, ZH ; partis politiques : PLR, PS ; Organisations : ASB, asut, CFF, Coop, DFS, digitalswitzerland, economiesuisse, EXPERTsuisse, FMH, H+, HKBB, IGEM, la Poste, les banques domestiques, Migros, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim, Raiffeisen, Ringier, santésuisse, Scienceindustries suisse, SDV, SPA, Sunrise UPC, suva, SWICO, thurbo, UBCS, UTP, veb.ch, VUD, Walderwyss. Selon swissICT, la confidentialité, l'intégrité, la disponibilité et la traçabilité devraient figurer, à tout le moins, dans les commentaires du rapport explicatif relatifs à l'art 2 ; personne privée : Beat Lehmann propose de créer un alinéa 1 « généralités », qui reprendrait la confidentialité, l'intégrité, la disponibilité et la traçabilité comme objectifs à atteindre.

93 Organisation : FSA.

94 Organisations : ASB, asut, digitalswitzerland, economiesuisse, Forum PME, HKBB, la Poste, les banques domestiques, Raiffeisen, Scienceindustries suisse, SDV, Sunrise UPC, SWICO.

contraire à la volonté du législateur[95]. Pour SPA, une telle documentation n'est pas légitime ; du moins, elle se justifie uniquement de manière brève pour le processus et son résultat. La reprise des objectifs figurant dans l'OLPD actuelle est critiquée[96]. Ces derniers sont vus comme obsolètes par certains[97]. DFS considère qu'un apport pratique d'experts dans le domaine de l'information et de la protection des données est indispensable dans le cadre de la révision de ladite disposition.

Selon quelques participants[98], l'art. 2 ne remplit pas complètement le mandat institué par l'art. 8, al. 3, nLPD. Divers participants[99] font remarquer que la disposition ne devrait mentionner que les objectifs de protection sur lesquels le responsable peut exercer une influence. Ils indiquent que l'introduction du « privacy by design » fait peser sur le responsable la charge de la sécurité des données. Eu égard aux avancées technologiques et en l'absence de toute intervention étatique, l'énumération doit être revue. Elle fait peser les efforts en matière de sécurité des données sur l'exploitant et non sur le développeur de technologies de l'information, et ce au détriment des utilisateurs de technologies de l'information. Les cyberattaques actuelles rendent irréalistes des objectifs aussi larges et ambitieux, notamment à la lumière des sanctions pénales de la nLPD[100].

Quelques participants[101] se demandent s'il ne faudrait pas préciser le lien avec l'art. 1, à tout le moins, que seuls doivent être mis en œuvre les éléments nécessaires pour garantir une sécurité appropriée des données.

BE est d'avis que la phrase introductive doit préciser « les mesures techniques et organisationnelles ». Une grande majorité de participants[102] proposent de remplacer « atteindre » par « s'efforcer de », notamment eu égard à l'art. 61, let. c, nLPD. Le PVS relève que les objectifs ne doivent être atteints que « dans la mesure du possible », laissant aux responsables une marge d'appréciation pouvant aller à l'encontre de la sécurité des données. Datenschutzguide.ch estime que ce complément circonstanciel est central. La mise en œuvre de nombreux objectifs peut être délicate pour les PME. L'accent doit être mis sur des exigences minimales. Il ne peut s'agir d'un catalogue détaillé passible d'amendes. Quelques participants[103] considèrent que ladite locution est inutile au vu de l'art. 6, al. 5, nLPD, d'autant qu'elle tend à relativiser les objectifs à atteindre. Divers participants[104] proposent la suppression de celle-ci, étant sujette à interprétation. Deux participants[105] appellent à plus d'explication autour de l'expression « dans la mesure du possible », le rapport explicatif n'étant pas d'un grand secours.

---

95 Organisations : Association de commerce, Coop, IGEM, la Poste, suva, Rega, VUD. Certains, dont la SPA, expliquent que tous ces objectifs ne sont pas nécessairement pertinents. Partant, il doit être possible de déterminer, sur la base du traitement, quel objectif est pertinent et lequel ne l'est pas.

96 À ce sujet, voir notamment nbp n. 50.

97 Organisations: DFS, IGEM.

98 Parti politique: PLR; organisations : Datenschutzguide.ch, Forum PME, SPA, suisa, SwissFoundations.

99 Organisations: ASP, Creditreform, EPS, FSEP, usam, vsi.

100 Parti politique : PLR ; organisations : la Poste, rega.

101 Canton : BE ; organisations : ASB, ASDPO, Association de commerce, digitalswitzerland, economiesuisse, HKBB, la Poste, les banques domestiques, Raiffeisen, Scienceindustries suisse, SDV, swissICT.

102 Canton : BE ; organisations : ASP, asut, CFF, Coop, Creditreform, DigiGes, EPS, FSEP, GastroSuisse, H+, IGEM, la Poste, Migros, Raiffeisen, Ringier, santésuisse, SSMD, SPA, Stiftung für Konsumentenschutz, Suisa, Sunrise UPC, suva, SWICO, swissICT, swissstaffing, thurbo, UTP, VUD, Walderwyss.

103 Parti politique: PS ; organisations : Stiftung für Konsumentenschutz, USS.

104 Parti politique : PS ; organisations: ASDPO, DigiGes, FRC, PES, PPS.

105 Organisations : CFC, DigiGes.

Swimag juge pertinent d'ajouter « au moins » devant « les objectifs de protection suivants ». GR propose plutôt d'ajouter « notamment » afin de ne pas comprendre la liste de manière exhaustive. DFS est d'avis qu'une liste exhaustive n'a pas de sens, dès lors qu'il s'agit ici de mesures techniques et organisationnelles, et non d'objectifs. Le PPS souhaite l'introduction d'une distinction entre les entreprises pour lesquelles le traitement des données n'est que de nature administrative et les entreprises dont le modèle d'affaires est basé sur la collecte, l'analyse, la mise à disposition et/ou l'utilisation des données. Pour pallier tout abus, ces dernières entreprises devraient voir cette marge d'appréciation davantage limitée.

Selon les banques domestiques, la réalité du marché économique suisse appelle à plus de précision.

Les objectifs de protection doivent être appréhendés selon leur contexte et par rapport au niveau de sensibilité des données[106]. La formulation doit permettre de comprendre qu'une approche tendant vers ces objectifs est suffisante. Il s'agit d'objectifs généraux, dès lors que le risque zéro n'existe pas[107]. Dans cet ordre d'idées, le rapport explicatif contient une liste d'objectifs de protection sur lesquels les mesures doivent se concentrer. Force est de constater que chaque objectif de protection n'est pas pertinent dans tous les cas et doit être adapté[108]. Une nouvelle structure faciliterait peut-être cette compréhension. HÄRTING propose d'introduire un alinéa « généralité »[109] et un alinéa « moyen de mise en œuvre des objectifs », qui serait une clause générale indiquant les mesures organisationnelles et techniques dont disposeraient les responsables du traitement ou les sous-traitants pour atteindre les objectifs de protection et où les moyens appropriés seraient recensés.

Ringier recommande d'intégrer dans l'ordonnance le catalogue des objectifs (intégrité, confidentialité et disponibilité), dès lors que la violation des exigences en matière de protection des données peut entraîner des conséquences notables (sanctions pénales selon l'art. 61, let. c, nLPD).

HÄRTING suggère d'ajouter, notamment dans une nouvelle lettre j, une obligation de rendre des comptes au sein de l'entreprise en cas de non-respect de ces objectifs ; et dans une nouvelle lettre m prévoir un contrôle continu de l'amélioration de la sécurité des données tenant compte de l'évolution constante de la technique.

Titre

Bär & Karrer propose de modifier le titre de l'art. 2 par la formule suivante : « exigences minimales ».

Let. a

Selon Swimag, l'expérience montre que le nombre de personnes autorisées a tendance à augmenter sans raison apparente, notamment pour des traitements n'entrant pas dans le cadre de leurs tâches. Partant, il est d'avis que la let. a devrait préciser que le nombre des personnes autorisées est réduit au minimum. Il sied également d'ajouter que l'accès est limité aux données dont elles ont « absolument et impérativement » besoin.

[106] Organisation : Classtime.

[107] Organisations : ASP, BNS, Creditreform, EPS, FSEP, usam, vsi ; personne privée : Beat Lehmann.

[108] Organisation : HÄRTING.

[109] À ce sujet, voir nbp n. 92.

Let. b

Selon la suva, les installations « mobiles » sont également concernées, notamment les smartphones et tablettes. Quand bien même ASA reconnaît que c'est la vision amenée par le rapport explicatif, elle est d'avis que ce type de contrôle n'est pas possible et relève simplement du contrôle de la let. a. Une clarification, notamment dans le rapport explicatif, est demandée[110]. La formule est jugée trop large et irréaliste (par exemple avec le télétravail lors de la pandémie). Il se justifie de mettre l'accent sur l'impossibilité pour les personnes non autorisées d'avoir accès.

Swimag propose de compléter le texte de la manière suivante : « l'accès aux locaux et aux installations physiques et virtuelles […] est d'emblée et dès le départ refusé […] ».

Let. c, d, e

Un petit nombre de participants[111] proposent de remplacer l'énumération de verbes (lire, modifier, déplacer, etc.) par le verbe « traiter ». Ils demandent plus de précision, notamment qu'une distinction soit réalisée entre support de données (let. c) et mémoire (let. d). Selon l'ASA, il importe de déterminer si le traitement se rapporte au support de données ou aux données qui y sont contenues. Swimag souhaite également plus de précision et suggère l'ajout de « décrire et détériorer » à la let. c devant « ou supprimer ».

DFS considère que déclarer à la let. c que les personnes non autorisées « ne peuvent pas » n'est pas suffisant. Le contrôle des supports de données doit « garantir » cela.

L'ASDPO propose de remplacer « mémoire » par « intégrité » à la let. d. Ce dernier terme semble plus adapté à la situation.

Let. g

La disposition doit éviter l'introduction de nouvelles notions non définies dans la nLPD ni dans le rapport explicatif : notamment le « système automatisé »[112].

La suva est d'avis que le contrôle de toute modification doit pouvoir intervenir *a posteriori*.

Selon Swimag, le système automatisé doit pouvoir réaliser des vérifications « à tout moment ». Le texte doit être complété de la manière suivante : le « but ainsi que du fondement légal de la saisie ou de la modification ».

Let. h

La suva est d'avis que la possibilité d'identifier l'organe est suffisante. Un participant[113] ajoute, néanmoins, que la vérification doit pouvoir intervenir « à tout moment ».

[110] Organisations : ASA, curafutura.

[111] Organisations : ASA, curafutura, santésuisse.

[112] Organisation : Association de commerce.

[113] Organisation : Swimag.

Let. i

La suva soulève l'utilité d'élaborer un concept de sauvegarde. Selon Swimag, en sus d'incident physique ou technique, tout autre danger pour les données doit être envisagé. La restauration doit être intégrale, immédiate et sans aucun préjudice.

Let. j

Selon l'Association de commerce, cette lettre doit être supprimée, étant irréaliste. Aucune entreprise ne peut garantir la disponibilité en tout temps de service Cloud, le signalement automatique d'erreurs par des logiciels, etc.

Tout dysfonctionnement doit automatiquement être signalé par le système[114].

Let. k

La détection doit pouvoir être « immédiate » et les mesures être prises « avec succès et intégralement »[115].

3.2.3 Art. 3 P-OLPD : Journalisation

La disposition est saluée par plusieurs participants[116]. Elle est même vue comme très importante, voire comme l'avenir du noyau de la protection des données en Suisse[117]. DigiGes relève que cette disposition s'appuie sur une base légale suffisante. La journalisation ne vise que des traitements de données présentant un risque élevé : une entreprise qui effectue de tels traitements est tenue d'assurer une protection élevée. H+ estime qu'une obligation ponctuelle de journalisation peut être pertinente (p. ex. pour évaluer des logs). GL salue l'introduction « d'exigences plus strictes » à l'alinéa 2. Non seulement cela renforce la confiance dans les traitements réalisés par les organes publics, de plus cette obligation permet un contrôle efficace. L'obligation de journalisation doit, en outre, avoir un certain effet préventif.

Cet article fait aussi l'objet d'un très grand nombre de critiques. La principale s'attache au défaut de base légale et au besoin de précision. Selon plusieurs participants[118], l'art. 8 nLPD traite de la sécurité des données au sens strict et ne serait pas suffisant pour fonder l'obligation de journalisation. Par ailleurs, le terme « journalisation » ne figure que dans le texte de l'ordonnance et non dans la nLPD, au contraire de la loi fédérale du 25 septembre 2015 sur le renseignement[119] ou encore de la loi fédérale du 28 juin 1967 sur le contrôle des finances[120]. Partant, la journalisation est perçue comme un Swiss Finish, également absent du RGPD. La journalisation crée un surplus de travail considérable. La suppression de l'article

[114] Organisation : Suva.

[115] Organisation : Swimag.

[116] Canton : GL ; Partis politiques : PS ; PVS.

[117] Parti politique : PVS ; organisation : FRC souligne également le rôle important de cette disposition pour la sécurité des données.

[118] Canton : ZH ; organisations : AFBS, ASA, ASB, ASP, ASPS, ASSL, Association de commerce, asut, auto suisse, BNS, CFC, CFF, Coop, Creditreform, curafutura, CURAVIVA.CH, Datenschutzguide.ch, DFS, digitalswitzerland, economiesuisse, EPS, EXPERTsuisse, FSA, FSEP, H+, HKBB, HotellerieSuisse, IGEM, INSOS, IS, la Poste, les banques domestiques, Migros, Raiffeisen, rega, Ringier, santésuisse, Scienceindustries suisse, SDV, senesuisse, SPA, SPITEX suisse, suva, SWICO, Swiss Insights, Swissholdings, swissICT, Swissstaffing, thurbo, UPSA, usam, UTP, UVS, veb.ch, vsi, VUD, Walderwyss. L'ATPrD est d'avis que le renvoi entre la nLPD et l'ordonnance n'est pas toujours aisé à comprendre, voire est contradictoire ; parti politique : le Centre.

[119] LRens, RS **121**, not. l'art. 78, al. 5.

[120] LCF, RS **614.0**, not. l'art. 10, al. 3.

est demandée, à tout le moins pour le domaine privé[121]. Avec l'introduction de l'analyse d'impact relative à la protection des données (AIPD) et l'utilisation du registre des activités de traitement, la journalisation est vue comme un doublon non indispensable. La journalisation serait, en outre, contraire à la volonté du législateur[122]. H+ déclare qu'une norme générale obligeant la journalisation est disproportionnée.

Plusieurs participants[123] font remarquer que le but de la journalisation est de permettre, lorsqu'un traitement non autorisé ne peut d'emblée être techniquement exclu, de constater *a posteriori* un traitement non autorisé. Ainsi l'évaluation des risques ainsi que la planification des mesures fondent le besoin de journalisation. Un risque hypothétique n'est ni suffisant ni proportionné. Cela doit être déterminé dans le cadre d'une investigation conforme à un art. 1 ayant été adapté. Il sied de souligner que la journalisation résulte de mesures techniques et/ou organisationnelles non suffisantes ou efficaces. Le rapport explicatif précise que la journalisation est un moyen pour atteindre les objectifs de l'art. 2. Il est demandé que soit précisé si la journalisation doit être mise en place en l'absence d'une analyse d'impact relative à la protection des données (AIPD). Certains participants[124] considèrent comme suffisante une journalisation lorsqu'il ne serait pas possible de déterminer *a posteriori* si les données ont été traitées dans le but pour lequel elles ont été collectées ou communiquées (art. 10, al. 1, OLPD). Divers participants[125] insistent sur le fait que pour découvrir des fuites de données non autorisées, des logiciels malveillants, des intrusions, etc., la journalisation de l'utilisation régulière des données n'est pas d'un grand secours.

Pour certains participants[126], conformément à l'art. 8 nLPD, une mise en œuvre de la protection des données axée sur les besoins et adaptée à l'état le plus récent de la technique est attendue. Cela est néanmoins délicat à mettre en pratique ; notamment avec une disposition présentant un tel niveau de détails, qui entraîne des frais de mise en œuvre élevés, un manque de clarté et des risques de confusion. Ils sont, toutefois, d'avis que la journalisation est la bonne solution, dans la mesure où aucune autre mesure ne permet d'atteindre le même objectif à moindre coût. Elle devrait, à tout le moins, être expressément prévue comme mesure dans l'ordonnance, voire sa ou ses alternatives. ZH précise que la journalisation, en cas de risque élevé, est contradictoire avec le refus de fixer des mesures concrètes. D'après un faible nombre de participants[127], l'obligation doit être limitée aux cas représentant un risque (résiduel) élevé, voire quand la mesure est adaptée au sens de l'art. 1. Par conséquent, les textes français et italien doivent être adaptés en ce sens. Le respect de la disposition présente des difficultés pratiques, notamment en raison des sanctions pénales (art. 61, let. c, nLPD), qui seront certainement nombreuses. Quelques participants[128] soulèvent un risque de surveillance des personnes concernées qui ne se justifie que si le traitement présente un risque élevé.

---

[121] Organisations: ASSL, auto suisse, HotellerieSuisse, Swiss Insights, UPSA.

[122] Organisations : ASB, ASP, ASSL, Association de commerce, asut, auto suisse, Bär & Karrer, BNS, CFC, CFF, Coop, Creditreform, digitalswitzerland, economiesuisse, EPS, EXPERTsuisse, FSEP, H+, HKBB, IGEM, la Poste, les banques domestiques, Migros, Raiffeisen, rega, Ringier, SDV, santésuisse, Scienceindustries suisse, suva, SWICO, Swissholdings, Swiss Insights, thurbo, UPSA, usam, UTP, vsi, VUD, Walderwyss.

[123] Cantons : AG, AR, BE, GL, GR, NW, VD, ZH ; organisations : ASB, CFF, Coop, digitalswitzerland, economiesuisse, FMH, FRC, FSA, H+, HKBB, IGEM, la Poste, les banques domestiques, Migros, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim, Raiffeisen, Ringier, santésuisse, Scienceindustries suisse, SDV, suva, thurbo, UPSV, UTP, VUD, Walderwyss.

[124] Organisations : ASSL, auto suisse, Bär & Karrer, Swiss Insights, UPSA.

[125] Organisations : CFF, H+, IGEM, la Poste, Migros, Ringier, santésuisse, suva, thurbo, UTP, VUD, Walderwyss.

[126] Organisations : ASPS, CURAVIVA.CH, HÄRTING, INSOS, IS, senesuisse, SPITEX suisse, swissICT.

[127] Organisations : AFBS, CFF, Classtime, HDC, la Poste, swissprivacy.law, thurbo, UTP.

[128] Organisations : Creditreform, DigiGes, FRC, vsi.

Al. 1

La révision de cet alinéa est demandée. Plusieurs participants[129] déclarent que l'analyse d'impact relative à la protection des données (AIPD) ne révèle pas un risque élevé en raison d'une sécurité insuffisante des données, mais en raison de la manière dont les données sont traitées. Partant, quelques participants[130] sont d'avis que l'AIPD ne concerne pas la sécurité des données.

Selon divers participants[131], il sied de renoncer à l'enregistrement de la lecture, qui n'est guère réalisable. Pour Swimag, il importe d'ajouter « ainsi que la finalité ou le motif précis du traitement » à la dernière phrase.

Quelques participants[132] se demandent si la notion de « traitement automatisé » ne devrait pas être définie. De l'avis de quelques participants[133], il sied de comprendre la notion *a contrario*, c'est-à-dire comme concernant les traitements autres que manuels. En d'autres termes, il s'agit d'un traitement électronique, voire de tous les traitements qui lui sont comparables.

Al. 2

Un certain nombre de participants[134] s'opposent à une obligation générale de journalisation pour les organes fédéraux, celle-ci étant contraire au principe de la proportionnalité. Pour quelques participants[135], quand bien même le respect de l'art. 25 de la Directive (UE) 2016/680 impose l'élaboration d'une disposition au niveau helvétique, celle-ci devrait être limitée aux organes fédéraux qui y sont soumis. À défaut, l'art. 3, al. 1, est applicable. Certains participants[136] rappellent que l'art. 57l, let. b, ch. 4, de la loi fédérale du 21 mars 1997 sur l'organisation du gouvernement et de l'administration[137] autorise l'enregistrement de données secondaires pour retracer l'accès lorsque l'enregistrement est proportionné. Le fait que même les données personnelles simples doivent faire l'objet d'une journalisation va clairement au-delà de cette exigence. Quelques participants[138] proposent d'inclure les organes fédéraux à l'alinéa 1 et supprimer l'alinéa 2. Divers participants[139] rappellent, en outre, que la journalisation existe indépendamment de tout risque. Elle est effectuée pour chaque traitement automatisé.

[129] Organisations : CFF, Coop, EXPERTsuisse, H+, IGEM, Migros, Ringier, santésuisse, suva, swissICT, thurbo, UTP, VUD, Walderwyss.

[130] Organisations : CFF, Coop, H+, IGEM, Migros, Ringier, suva, thurbo, UTP, VUD, Walderwyss.

[131] Organisations : BNS, CFF, curafutura, H+, IGEM, la Poste, Migros, Ringier, santésuisse, suva, swissICT, thurbo, UTP, VUD, Walderwyss.

[132] Organisations : Association de commerce, BNS, CFF, H+, HDC, IGEM, la Poste, Migros, Ringier, santésuisse, suva, swissICT, thurbo, UTP, VUD, Walderwyss.

[133] Organisations : CFF, H+, IGEM, la Poste, Migros, Ringier, santésuisse, suva, thurbo, UTP, VUD, Walderwyss.

[134] Cantons : GR, NW, SH, SO, VD ; organisations : CFF, curafutura, HDC, IGEM, la Poste, Préposé à la protection des données de SZ, OW et NW, privatim, Ringier, santésuisse, suva, swissICT, thurbo, UTP, VUD.

[135] Canton : SH ; organisations : CFF, curafutura, HDC, la Poste, thurbo, UTP.

[136] Cantons : AR, BE, GL, NW ; organisations : ATPrD, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim.

[137] LOGA, RS **172.010**.

[138] Cantons : AR, BE, GL, NW, SO ; organisations : ATPrD, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim.

[139] Organisations : CFF, H+, IGEM, la Poste, Migros, Ringier, santésuisse, suva, thurbo, UTP, VUD, Walderwyss.

Des participants[140] sont d'avis que le régime devrait, au moins, être le même pour les personnes privées et les organes fédéraux.

Pour Swimag, il importe d'ajouter « ainsi que la finalité ou le motif précis du traitement » à la dernière phrase.

Al. 3

Dès lors que tout traitement n'inclut pas forcément une communication, quelques participants[141] sont d'avis qu'il serait de l'ordre du raisonnable d'introduire « le cas échéant » devant « l'identité du destinataire ».

Selon quelques participants[142], cet alinéa contredit les deux alinéas précédents. L'idée exprimée semble être que la journalisation serve à mettre en évidence les traitements non autorisés, qui ne seraient pas constitutifs d'une violation de la sécurité des données. Il se justifie de préciser que le terme « destinataire » désigne l'organisation et non l'individu.

De l'avis de deux participants[143], la journalisation est une documentation qualifiée qui conduit à un profilage. Il est possible d'établir qui, quand, comment et dans quelle mesure des données ont été traitées. Il s'agit d'un traitement qualifié et automatisé des données de la personne qui a traité les données. Une base légale au sens formel est dès lors indispensable, essentiellement si dans le cadre professionnel la journalisation devait permettre un véritable profilage et un contrôle du comportement de l'employé.

Al. 4

Quelques participants[144] sont favorables au maintien du délai de conservation actuel de 1 an. Ils sont d'avis de s'inspirer du § 5 de l'ordonnance relative à la loi sur l'information, la protection des données et les archives du canton d'Argovie[145]. Pour un grand nombre de participants[146], le défi que représente l'augmentation des cyberattaques contredit toute prolongation de la durée de conservation. Au lieu de permettre une évaluation plus judicieuse, cette prolongation engendrerait inutilement des coûts et efforts supplémentaires sans pour autant atteindre un niveau plus élevé de protection. Une conservation séparée n'aurait pas un meilleur résultat. Une protection accrue contre toute modification subséquente aurait plus de portée. La conduite d'une telle procédure de séparation implique également un risque pour la sécurité des données. La durée de conservation doit être conçue comme un minimum approprié et non rigide. La durée de deux ans est jugée inappropriée. ZH déclare qu'une conservation de quelques jours, voire de quelques mois, est seule appropriée. economiesuisse est d'avis que la durée de conservation devrait dépendre de celle du traitement. Deux participants[147]

[140] Orgnisations : ASDPO, swissICT.

[141] Cantons : AG, AR, BE, GL, NW, VD ; organisations : ATPrD, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim.

[142] Organisations : CFF, H+, IGEM, la Poste, Migros, Ringier, santésuisse, suva, thurbo, UTP, VUD, Walderwyss.

[143] Organisations : Creditreform, VSI.

[144] Canton : GL ; organisations : asut, curafutura, Sunrise UPC, SWICO, swissICT.

[145] VIDAG, SAR 150.711.

[146] Cantons : GL, TG, ZH ; organisations : ASDPO, ASP, ASPS, ASSL, Association de commerce, asut, auto suisse, Bär & Karrer, CFF, Creditreform, curafutura, CURAVIVA.CH, EPS, FMH, FSEP, H+, INSOS, IS, la Poste, rega, Ringier, senesuisse, SPITEXsuisse, SSMD, Sunrise UPC, suva, SWICO, Swimag, Swiss Insights, thurbo, UPSA, usam, UTP, veb.ch, vsi, VUD, Walderwyss. ASDPO et Bär & Karrer proposent d'harmoniser tous les délais de l'ordonnace. Swimag propose un délai uniforme de cinq ans.

[147] Parti politique : PS ; organisation : USS.

sont, au contraire, satisfaits et soutiennent le délai de conservation de deux ans. Des participants[148] considèrent que cette obligation conduit à l'élaboration de bases volumineuses de données avec de longues durées de conservation (par exemple : les données des utilisateurs/collaborateurs, etc.). Quelques participants[149] proposent la suppression de la conservation séparée.

Divers participants[150] rappellent que, pour les organes fédéraux, l'art. 57m ss LOGA et son ordonnance sur l'organisation du gouvernement et de l'administration[151] définissent la procédure. Une évaluation personnelle n'est pas toujours nécessaire. Il sied d'ajouter à la dernière phrase de cet alinéa : « ils ne sont utilisés qu'à cette fin et à des fins personnelles que dans la mesure où cela est nécessaire ». La limitation de l'accès ainsi que celle de la finalité sont jugées trop strictes. D'autres raisons pourraient justifier la consultation des logs, notamment par le responsable ou le sous-traitant. Il sied de veiller à éliminer les doublons. La disposition devrait émettre une réserve pour les dérogations contenues dans la législation sectorielle. L'alinéa doit être supprimé, voire le cercle des personnes ayant accès doit être élargi.

Quelques participants[152] sont d'avis que la formule « séparément du système dans lequel les données personnelles sont traitées » est à remplacer par « sécurisé ».

3.2.4 Art. 4 P-OLPD : Règlement de traitement des organes fédéraux

Plusieurs participants[153] saluent expressément cette disposition. Elle est vue comme une pièce maîtresse pour le futur du droit de la protection des données. D'autres participants[154] aimeraient même étendre sa portée, car les critères de l'alinéa 1 sont jugés arbitraires et ne couvrant pas tous les traitements critiques. La mesure est admise, mais appelle quelques précisions. On y voit une mesure favorisant la minimisation des données[155] et on estime justifié que lors de traitements présentant un risque élevé, comme le traitement de données sensibles ou le profilage, des exigences plus élevées soient prévues[156].

Pour de nombreux autres participants[157] la disposition serait en revanche contraire à la volonté du législateur et redondante. De l'avis d'un grand nombre de participants[158], concernant l'obligation de documentation, il a été décidé de se limiter au registre des activités de traitement, voire à l'analyse d'impact relative à la protection des données (AIPD). Les critiques soulignent ainsi l'absence de base légale. Partant, le règlement de traitement ne sert pas

[148] Cantons : BL, ZH. Selon BL, c'est l'obligation générale de journalisation qui mène à la création de base de données volumineuses.

[149] Cantons : TG, ZH ; organisations : Association de commerce, ASSL, auto suisse, Classtime, CFF, Creditreform, H+, la Poste, Migros, rega, Ringier, SPA, suva, Swiss Insights, thurbo, UPSA, UTP, vsi, VUD, Walderwyss.

[150] Cantons : AG, AR, BE, GL, NW, SH, VD ; organisations : ATPrD, Migros, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim, UVS, VUD.

[151] OLOGA, RS **172.010.1**.

[152] Organisations : CFF, H+, IGEM, la Poste, Migros, Ringier, suva, thurbo, UTP, VUD, Walderwyss.

[153] Partis politiques : PS, PVS ; organisation : DigiGes.

[154] Cantons : AG, AR, BE, GL, GR, NW, SH, SO, SZ, UR, VD, ZH ; parti politique : PVS ; organisations : ATPrD, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim.

[155] Parti politique : PS.

[156] Organisation : DigiGes.

[157] Organisations : ASA, ASB, asut, BNS, CFF, curafutura, DFS, economiesuisse, EXPERTsuisse, Forum PME, H+, HKBB, IGEM, la Poste, les banques domestiques, proFonds, santésuisse, Scienceindustries suisse, SDV, Sunrise UPC, suva, SWICO, swissICT, thurbo, UBCS, UTP, VUD, Walderwyss.

[158] Cantons : AR, BE, GL, GE, TG ; organisations : ASB, ASA, ASDPO, ASSL, asut, ATPrD, auto suisse, BNS, CFF, Coop, Creditreform, curaturura, DFS, digitalswitzerland, economiesuisse, EXPERT suisse, H+, HÄRTING, HDC, HKBB, HotellerieSuisse, IGEM, la Poste, les banques domestiques, Migros, pharmasuisse, Préposé cantonal à la protection des données et à la transparence NE/JU, proFonds, Raiffeisen, rega, Ringier, Scienceindustries suisse, SDV, SSMD, Surnrise, UPC, suva, SWICO, swissICT, SwissHoldings, Swiss Insights, Swissstaffing, thurbo, UPSA, UTP, vsi, VUD, Walderwyss. privatim demande tout particulièrement que l'alinéa 3 soit supprimé. À ce sujet, voir nbp n. 176 ; parti politique : PLR.

à garantir la sécurité des données au sens strict (qui relève de l'art. 8 nLPD), mais assure le respect des principes et prescriptions en matière de protection des données. Ils relèvent que le RGPD n'en fait aucune mention, quand bien même l'obligation de documentation en découle. Ils critiquent ce Swiss Finish. La suppression de cette disposition est demandée. Divers participants[159] sont d'avis que cette obligation contredit l'approche basée sur le risque. Certains participants[160] rappellent que l'art. 11a LPD n'a volontairement pas été repris, comme l'explique le rapport explicatif.

Pour plusieurs participants[161], le cadre légal est le suivant : l'art. 36 LPD offre la possibilité d'établir un « règlement de traitement », alors que l'art. 12 nLPD introduit la notion de « registre des activités de traitement ». Ils sont d'avis que le système semble avoir remplacé le règlement par le registre. Il est souligné que les art. 1 et 2 ne mentionnent pas le règlement de traitement parmi les mesures. La valeur ajoutée de cet instrument en termes de transparence est discutable ; d'autant plus avec l'introduction du registre des activités des traitements. Au même titre que la journalisation des droits d'accès, voire des accès, les mesures techniques ou organisationnelles sont des obligations. Des précisions demeurent nécessaires pour éviter des doublons inutiles ainsi qu'un surcroît de travail non indispensable. Des participants[162] déclarent que le règlement de traitement est inutile et, au contraire, créerait même un risque pour le responsable si les personnes concernées tentent de l'obtenir par le biais du droit d'accès. En effet, certaines informations figurant dans le règlement relèvent du devoir d'informer.

Deux participants[163] sont d'avis que, à tout le moins, le champ d'application et la nécessité doivent être précisés, notamment pour les entreprises unipersonnelles.

Divers participants[164] jugent utile de rappeler que l'obligation d'établir un règlement de traitement n'est pas nouvelle et figure dans le texte actuel de l'ordonnance. Ils déclarent qu'au vu du choix opéré pour une limitation de l'obligation de documentation et d'information (AIPD, registre des activités de traitement ou déclaration de confidentialité), la suppression dans la nouvelle mouture semblait attendue.

Al. 1

Limiter l'établissement d'un règlement de traitement aux données sensibles à grande échelle ou aux profilages à haut risque est pour plusieurs participants[165] arbitraire, voire trop restreint. À l'image de l'art. 22, al. 1, nLPD, l'approche basée sur le risque ne justifie pas un tel raisonnement. Les lettres a et b doivent être comprises comme des exemples non exhaustifs qui présentent toujours un risque élevé. Cette restriction (let. a et b) ne permet pas de couvrir les traitements de données critiques pour les droits de la personnalité. La reprise des conditions de l'analyse d'impact relative à la protection des données (AIPD) (art. 22, al. 1, nLPD) est,

[159] Organisations : ASSL, auto suisse, Raiffeisen, Swiss Insights, UPSA.

[160] Organisations : HotellerieSuisse, proFonds, Raiffeisen.

[161] Parti politique : PLR ; Organisations : ASB, ASA, asut, Bär & Karrer, BNS, CFF, curafutura, digitalswitzerland, economiesuisse, H+, HDC, HKBB, HotellerieSuisse, la Poste, les banques domestiques, Migros, Raiffeisen, rega, Ringier, santésuisse, Scienceindustries suisse, SDV, suisa, Sunrise UPC, suva, SWICO, SwissHoldings, thurbo, UTP, veb.ch, VUD, Walderwyss.

[162] Organisations : ASA, Coop, curafutura, H+, IGEM, Migros, Raiffeisen, rega. CFF, Ringier, suiva, suva, thurbo, UTP, VUD et Walderwyss sont également d'avis que certains seraient tentés d'obtenir le règlement par la demande d'accès.

[163] Organisations : Creditreform, vsi.

[164] Organisations : ASSL, auto suisse, CFF, Coop, H+, la Poste, Migros, Ringier, suva, Swiss Insights, thurbo, UPSA, UTP, VUD. À l'exception de Coop, ils rappellent, concernant la journalisation (art. 3), que l'obligation de documenter a été supprimée au profit de celle de tenir un registre des activités de traitement

[165] Cantons : AG, AR, BE, GL, GR, NW, SH, SO, SZ, UR, VD, ZH ; parti politiques : PVS ; organisations : ATPrD, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim.

de ce fait, proposée. Dans le cadre de l'AIPD, de nombreux documents sont réalisés (art. 22, al. 3, nLPD). Ces derniers peuvent faire partie du règlement de traitement. Plusieurs participants[166] font remarquer que selon l'alinéa 2 les informations essentielles sont de toute façon déjà documentées dans le cadre de l'AIPD, et le reste dans l'inventaire qui doit de toute façon être établi. Certains[167] se posent dès lors la question de la valeur ajoutée d'un tel règlement.

D'après divers participants[168], quand bien même, il existe une très faible probabilité de voir dans la pratique des règlements en raison d'un « profilage à haut risque », il se pose la question de savoir à quel moment des données sont traitées « à grande échelle ». En ressources humaines, la notion serait justifiée en cas de volume moyen ou important de données ; alors qu'en termes de bases de données bibliographiques, il semblerait que non. Sont, de la même façon, concernées les entreprises de médias qui publient des articles sur la politique et la société, s'agissant de données personnelles sensibles (opinions politiques, etc.). Il sied de reconnaître un besoin de clarification pour la pratique (cabinet médical, etc.). Swimag propose de supprimer « à grande échelle ». À son sens, c'est précisément dans le cas de traitements mineurs et isolés de données personnelles sensibles qu'une sensibilisation est nécessaire ; d'où le besoin d'établir un règlement de traitement y relatif. Il suggère également de s'en tenir au simple profilage, à la place de « profilage à risque élevé ». Selon Bär & Karrer, en pratique, les entreprises ont pris l'habitude d'établir des directives internes. Elles ne sont toutefois pas aussi détaillées que le propose l'art. 4. Ce nonobstant, il est plutôt éloigné de la pratique d'élaborer un tel règlement pour des processus de traitement automatisé des données qui sont soumis à des changements constants et qui sont régulièrement adaptés ou étendus. Quelques participants[169] rappellent également que les traitements de données particulièrement sensibles peuvent nécessiter une réglementation interne. Cet aspect est toutefois déjà suffisamment réglé par l'art. 7, al. 1, nLPD'. Des participants[170] soulèvent la grande latitude d'interprétation autour de l'expression « risque élevé ». Ils recommandent d'introduire un complément d'information dans le rapport explicatif.

Selon swissICT, le règlement de traitement étant une mesure organisationnelle et technique pour garantir la sécurité des données (conforme au principe de *privacy by design* et *by default*), des erreurs figurent dans les critères d'exclusion. Les risques élevés pour la personnalité sont mélangés avec des aspects de la sécurité des données (confidentialité, intégrité, disponibilité). La structure de cet alinéa est à repenser.

Al. 2

L'alinéa bénéficierait d'un renvoi vers les normes en matière de technologie de l'information. À tout le moins, une référence aux prescriptions spécifiques en matière de protection des données (let. h, j) serait judicieuse[171]. ZH ajoute qu'en présence d'une certification (par exemple : ISO 270001), il se justifie de renoncer à l'élaboration d'un règlement de traitement séparé.

[166] Organisations : CFF, H+, la Poste, Migros, Ringier, suva, thurbo, UTP, VUD, Walderwyss.

[167] Canton : BE ; organisations : ASA, ASSL, auto Suisse, curafutura, rega, Swiss Insights, UPSA, vsi.

[168] Orgnisations : ASB, Bibliosuisse, CFF, Coop, economiesuisse, ETH-Bibliothek, FMH, H+, HKBB, IGEM, la Poste, les banques domestiques, Migros, Raiffeisen, Ringier, Scienceindustries suisse, SDV, suva, thurbo, UTP, VUD, Walderwyss.

[169] Organisations : CFF, Coop, H+, IGEM, la Poste, Migros, Ringier, suva, thurbo, UTP, VUD, Walderwyss.

[170] Organisations: ASB, digitalswitzerland, economiesuisse, HKBB, la Poste, les banques domestiques, Raiffeisen, SDV, Scienceindustries suisse.

[171] Cantons : BE, GL, VD, ZH ; organisation : ATPrD, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim.

Divers participants[172] font remarquer que les lettres a, b, c et f font partie des indications devant figurer dans le registre des activités de traitement. Les autres lettres sont à prendre en compte dans l'analyse d'impact relative à la protection des données (AIPD) en cas de pertinence pour l'évaluation des risques ou en tant que mesure de réduction des risques. Il faut ainsi comprendre que la documentation a déjà lieu. Il ne s'agit apparemment pas juste de question de sécurité des données, mais bien du respect de la législation en matière de protection des données.

Selon quelques participants[173], il sied de préciser que les indications de cet alinéa ne doivent être fournies qu'en ce qui concerne les traitements qui relèvent de l'art. 1, al. 1, let. a et/ou b.

Divers participants[174] demandent que la liste soit réduite, car les exigences en cas de traitements de données sensibles sont trop lourdes, notamment pour les organismes des milieux médicaux. Les lettres d, e et j doivent être supprimées, car elles créent une charge administrative non indispensable. La lettre i doit être adaptée, car trop détaillée. Les lettres a, b, c, f et g sont saluées, étant des mesures centrales pour garantir la sécurité des données. Elles sont jugées suffisantes pour assurer le respect de la protection des données. La lettre h est également admise. PS considère le principe de minimisation des données comme essentiel en matière de protection des données. Dès lors, il salue vivement la lettre h.

Deux participants[175] demandent à être exclus expressément du champ d'application.

Al. 3

Plusieurs participants[176] sont d'avis que cet alinéa ne tient pas compte de la pratique. Le conseiller à la protection des données doit être un spécialiste. Le règlement de traitement est, de cette façon, établi avec lui et non mis à sa disposition sous une forme intelligible. L'une de ses tâches est de participer à l'application des prescriptions relatives à la protection des données (art. 10, al. 2, let. b, nLPD). En outre, le conseiller à la protection des données doit disposer des connaissances professionnelles nécessaires (art. 10, al. 3, let. c, nLPD). L'expression « sous une forme intelligible » semble méconnaître ce qui vient d'être souligné et doit être supprimée.

Divers participants[177] relèvent que le règlement ne doit ni être publié ni annoncé au PFPDT. L'introduction d'une présentation au conseiller ou à la conseillère à la protection des données est, ce faisant, contradictoire. Légalement, il n'y a aucune obligation d'instaurer cette fonction. Cette deuxième demi-phrase doit ainsi être supprimée. SO propose par exemple qu'il soit précisé dans le rapport explicatif que la désignation de celui-ci ou celle-ci est facultative.

Deux participants[178] sont d'avis que l'adverbe « régulièrement » nourrit une charge bureaucratique inutile, voire pousserait au non-respect de la règle. L'actualisation ne doit intervenir

[172] Organisations : CFF, H+, IGEM, la Poste, Migros, Ringier, suva, thurbo, UTP, VUD, Walderwyss

[173] Organisations : ASSL, auto Suisse, Swiss Insights, UPSA.

[174] Orgnisations : ASPS, CURAVIVA suisse, INSOS suisse, IS, senesuisse, SPITEX suisse.

[175] Organisations : Bibliosuisse, ETH-Bibliothek.

[176] Cantons : AR, BE, GL, NW, SH, SO, TG, UR, VD, ZH ; organisations : ATPrD, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim.

[177] Organisations : CFF, H+, Hotelleriesuisse, IGEM, la Poste, Migros, Ringier, santésuisse, suva, thurbo, UTP, VUD, Walderwyss.

[178] Organisations : Creditreform, vsi.

qu'en cas de besoin. D'autres participants[179] précisent que, à l'instar de l'art. 1, al. 2, les intervalles entre les mises à jour devraient être indiqués de manière plus précise, faute de quoi il existe un risque d'insécurité juridique et de litiges. Il est proposé de favoriser la formule : « au moins une fois par an ».

Swimag est d'avis que le libellé devrait s'adresser au responsable et au sous-traitant et non à la personne privée.

3.2.5 Art. 5 P-OLPD : Règlement de traitement des organes fédéraux

Dès lors que l'art. 4 et l'art. 5 traitent du règlement de traitement, nombre de participants[180] ont jugé pertinent d'opérer un renvoi vers les remarques faites sous l'art. 4. Il est simplement souligné que la réglementation est disproportionnée et qu'elle ne dispose pas d'une base légale. Le règlement de traitement serait notamment un doublon au registre des activités de traitement, voire à l'analyse d'impact relative à la protection des données (AIPD). La suppression de la disposition est demandée. Deux participants[181] font remarquer qu'une éventuelle suppression de l'art. 5 appellerait, à tout le moins, au besoin d'adaptation de l'art. 84b de la loi fédérale du 18 mars 1994 sur l'assurance-maladie[182].

Certains participants[183] soulignent que le champ d'application de la disposition est trop large pour les organes fédéraux. La Poste précise que l'obligation de réglementer tout profilage sans risque élevé demande de toute façon une base légale pour les organes fédéraux (art. 34, al. 2, let. b, nLPD). Sur la base de l'évaluation des risques effectuée par le législateur, des obligations réglementaires ponctuelles peuvent être fixées dans la législation sectorielle. Deux participants[184] rappellent qu'une bureaucratie excessive augmente l'utilisation inutile des ressources (en personnes et en argent) ; ce d'autant pour les organes fédéraux. Cette remarque s'applique de manière générale à l'ensemble du projet.

Al. 1 let. b

La notion étant très large, BE est d'avis que le profilage doit, à tout le moins, être compris, par analogie, dans les limites de l'art. 4, al. 1, let. b.

Al. 2

Certains participants[185] appellent à plus de clarté. La formulation laisse croire que le règlement pourrait contenir plus d'indications.

[179] Orgnisations : ASPS, CURAVIVA suisse, INSOS suisse, IS, senesuisse, SPITEX suisse.

[180] Cantons: AR, GL, NW, SH, SO, SZ, VD, ZH. BE propose autant la suppression de l'art. 4 que de l'art. 5 ; organisations : ASA, ASDPO, asut, ATPrD, CFF, curaturura, Datenschutzguide.ch, DFS, H+, HÄRTING, HDC, IGEM, la Poste, Migros, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim, Ringier, santésuisse, Sunrise UPC, suva, SWICO, swissICT, thurbo, UTP, VUD, Walderwyss.

[181] Organisations : curaturura, santésuisse.

[182] LAMal, RS **832.10**.

[183] Organisations : asut, BNS, CFF, H+, IGEM, la Poste, Migros, Ringier, Sunrise UPC, suva, SWICO, swissICT, thurbo, UTP, VUD, Walderwyss.

[184] Organisations : Creditreform, vsi.

[185] Organisations : CFF, H+, IGEM, la Poste, Migros, Ringier, suva, VUD, Walderwyss.

3.2.6 Art. 6 P-OLPD : Modalités

Certes, la disposition est saluée et jugée essentielle[186], mais elle également fortement critiquée. La suppression est demandée, à tout le moins certains alinéas, voire certaines phrases. De manière générale, l'adaptation du texte est sollicitée[187]. Un grand nombre de participants[188] soulèvent comme critique principale le défaut de base légale. Selon l'art. 9, al. 1, let. a, nLPD, le responsable doit veiller à ce que seuls soient effectués les traitements qu'il est lui-même en droit d'effectuer. L'« obligation, pour le responsable du traitement, de « s'assurer » que le traitement effectué par le sous-traitant est conforme au contrat et à la loi ne peut être suivie (art. 6, al. 1, 2ème phr., et art. 6, al. 2, 2ème phr). Cette répétition dans l'ordonnance ne se justifie pas, est disproportionnée et n'entre pas dans le cadre de la délégation au Conseil fédéral. De la nLPD, il ressort uniquement que l'organe public, voire la personne privée, demeure responsable de la protection des données. Le responsable du traitement doit, à tout le moins, s'assurer par la voie contractuelle qu'une protection des données équivalente est garantie. Il ne peut pas garantir, mais seulement « veiller à » (art. 9, al. 2, nLPD). Partant, le verbe « s'assurer » doit être adapté, voire remplacé par « veiller à ce que » ou « veiller de manière appropriée ». Il est proposé la formule rédactionnelle suivante : « aux termes de l'art. 9, al. 1, let. a, nLPD, le responsable doit veiller à ce que la LPD soit respectée ». SZ pense que ce procédé reviendrait à une surveillance permanente. Cette manière de faire n'est justement pas le sens et le but de l'externalisation d'activités administratives. Le responsable du traitement des données est clairement coresponsable du traitement des données conformément au mandat et à la loi.

Quelques participants[189] ne s'expliquent pas la raison qui a poussé à l'extension du champ d'application aux personnes privées, sachant que cet aspect ressort déjà de l'art. 9. Ils rappellent que l'art. 6, al. 1 et al. 2, est calqué sur l'art. 22 OLPD, qui ne s'appliquait qu'aux organes fédéraux. Lorsqu'un responsable confie le traitement à un sous-traitant à l'étranger, la LDP ne s'applique pas au sous-traitant. Il va de soi que le responsable doit respecter les règles des art. 16 à 18 nLDP. Le cas d'application dans lequel un sous-traitant étranger traite des données qui ne lui ont pas été transmises auparavant depuis la Suisse devrait être réglé à l'art. 16 nLPD et non pas dans le cadre de l'art. 6, al. 2.

Al. 1

TG salue le fait qu'un mandataire auquel il est fait appel doit garantir une protection des données équivalente. DigiGes salue également cet alinéa.

Certains participants[190] regrettent la fausse impression donnée par la première phrase selon laquelle la responsabilité du responsable n'est en aucun cas limitée. Il importe d'expliquer ce qu'il est entendu par le « responsable de la protection des données ». Dans l'hypothèse où une responsabilité civile serait entendue, cette responsabilité causale n'est pas prévue par le législateur. Ceci irait, en outre, au-delà de l'art. 82, ch. 3, RGPD. Sans oublier que l'art. 41 de

[186] Orgnisation : DigiGes.

[187] Canton : SZ ; organisations : ASB, ASDPO, ASP, ASSL, Association de commerce, asut, BNS, Bär & Karrer, Creditreform, DFS, EPS, FER, FSA, FSEP, GastroSuisse, HÄRTING, IGEM, la Poste, Raiffeisen, Ringier, SPA, suisa, Sunrise UPC, suva, SWICO, Swiss Insights, swissICT, Swissstaffing, UPSA, usam, vsi, VUD, Walderwyss.

[188] Canton : SZ ; organisations : ASB, ASP, ASSL, Association de commerce, asut, BNS, CFF, Creditreform, DFS, EPS, FER, FMH, FSEP, GastroSuisse, H+, HÄRTING, HotellerieSuisse, IGEM, la Poste, les banques domestiques, Migros, Raiffeisen, Ringier, SPA, suisa, Sunrise UPC, suva, SWICO, Swiss Insights, swissICT, Swissstaffing, thurbo, UPSA, usam, UTP, vsi, VUD, Walderwyss.

[189] Orgnisations : Bär & Karrer, swissICT.

[190] Organisations : ASB, asut, BNS, CFF, H+, IGEM, la Poste, les banques domestiques, Migros, Ringier, SPA, suisa, Sunrise UPC, suva, SWICO, swissICT, thurbo, UTP, VUD, Walderwyss.

la loi fédérale du 30 mars 1911 complétant le Code civil suisse[191] reste applicable à la responsabilité civile.

Concernant la seconde phrase, Curafutura s'interroge sur la nécessité de remplacer « conformément au mandat » par « conformément au contrat ou à la loi ». Avec d'autres participants[192], ils expliquent que le responsable ne peut pas garantir que le traitement soit conforme au contrat et à la loi. Il peut juste essayer de faire en sorte qu'il le soit comme pour l'art. 28, ch. 1, RGPD. En effet, dès que les données sont confiées à un sous-traitant, la garantie de la sécurité des données ne relève plus de la sphère d'influence du ou des responsables, voire leur influence est fortement limitée. Parmi les formules rédactionnelles, la suivante est proposée : « le responsable du traitement qui confie un traitement de données personnelles à un sous-traitant demeure responsable de la protection des données. Il veille à ce que les données soient traitées conformément au contrat ou à la loi ». À tout le moins, les responsables devraient être tenus de ne faire appel qu'à des sous-traitants ayant des mesures appropriées. Les explications apportées en lien avec l'art, 22, al. 3, de la directive (UE) 2016/680 n'apportent pas plus de clarté à l'art. 6. À l'image de l'art. 28, ch. 3, RGPD, il serait judicieux d'ajouter à l'art. 6 le contenu minimal obligatoire devant figurer dans les contrats de sous-traitance : soit l'objet, la durée, la nature et la finalité du traitement des données, le type de données personnelles, les catégories de personnes concernées ainsi que les obligations et les droits du responsable du traitement. Selon proFonds, il suffit que le responsable lie contractuellement les obligations légales au sous-traitant et l'incite ainsi à traiter les données conformément à la loi. Les petites ou moyennes structures et associations n'ont, en règle générale, ni la possibilité ni les ressources pour procéder à un contrôle complet. Dans cet ordre d'idées, il serait pertinent d'ajouter que le responsable doit aménager contractuellement les mandats de manière à ce qu'il soit conforme à la loi.

FSA se demande ce que l'on entend par un traitement conforme au contrat ou à la loi, dès lors que l'art. 9, al. 1, nLPD devrait couvrir cette question. Bär & Karrer propose de supprimer « au contrat ou ». Le PPS regrette une absence de définition claire de ce qu'il est entendu par « assurer un traitement au moins conforme au contrat ou à la loi ».

Pour TG, la formulation selon laquelle la protection des données doit être assurée par voie contractuelle lorsque la loi étrangère viole la protection des données en Suisse ne doit pas être maintenue. Il mentionne à titre d'exemple la loi chinoise sur le renseignement national, voire la législation américaine. Ces législations exigent des fournisseurs ayant un lien avec leur pays qu'ils divulguent aux autorités étrangères toute communication (électronique) ainsi que les enregistrements ou autres informations, y compris ceux situés en dehors de leurs frontières. Toute obligation contractuelle contraire à ces dispositions chinoises ou américaines a peu de chance d'être suivie.

Al. 2

D'après quelques participants[193], aux termes de l'art. 3 nLPD, il est peu probable qu'un sous-traitant ne soit pas soumis à la LPD. La suppression de cet alinéa ferait ainsi sens.

[191] Droit des obligations, CO, RS **220**.

[192] Organisations : ASA, ASSL, auto suisse, CFC, curafutura, FER, Gastrosuisse, HotellerieSuisse, santésuisse, SG, SSMD, Swiss Insights, UPSA.

[193] Organisations : ASDPO, HDC, swissprivacy.law.

Deux participants[194] considèrent que la liste des pays figurant dans l'annexe 1 de la nLPD s'applique.

Divers participants[195] déclarent que le sens et le but de cette lettre ne sont pas évidents. Le contenu est déjà couvert par les art. 16 et 17 nLPD. Dans ce sens, le rapport explicatif mentionne que l'art. 6, al. 2, correspond à l'art. 22, al. 3, OLPD actuelle. La seule nuance repose sur le fait que la disposition s'applique uniquement aux organes fédéraux, alors que l'art. 6, al. 2, concerne aussi bien les traitements effectués par des personnes privées que par des organes fédéraux. L'explication relative à cette délimitation fait défaut. La disposition semble trouver son sens dans des cas particuliers tels que les cas où un responsable suisse demanderait à un sous-traitant étranger de traiter des données sans qu'il y ait communication depuis la Suisse et que l'art. 16 nLPD ne s'appliquerait pas. D'un point de vue systématique, ce cas devrait toutefois être réglé à l'art. 16 nLPD et non dans l'ordonnance. Juridiquement, le fondement correct est l'art. 9, al. 1, let. a, nLPD. Dans le cas d'un traitement sur mandat, il s'agit de garantir que les données ne sont traitées que de la manière dont le responsable est autorisé à le faire ; ce que prévoit l'art. 9, al. 1, let. a, nLPD. Il est probable que la règle existante ait simplement été reprise. Partant, il est difficile de comprendre la nécessité de cet alinéa et sur quelle base juridique il se fonde.

Certains participants[196] demandent la suppression de cet alinéa en invoquant que la communication à l'étranger est déjà prévue par une autre disposition (art. 8). En outre, il ne peut être exigé du responsable de traitement de connaître toutes les législations pertinentes. Si cette réglementation devait être maintenue, ils suggèrent de préciser « qu'à défaut, une protection des données appropriée doit être mise en place ». Dans cet ordre d'idées, il serait judicieux de mentionner que si le sous-traitant n'est pas soumis à la LPD, le responsable doit s'assurer que d'autres dispositions légales garantissent une protection des données équivalente. Dans le cas contraire, il doit la garantir par voie contractuelle conformément à l'art. 16, al. 2, nLPD. Il serait toutefois préférable de supprimer cet alinéa.

Selon le PPS, à l'image de la nLPD, l'art. 6, al. 2, est dépassé non seulement à la lumière de la jurisprudence récente (notamment l'arrêt Schrems II de la CJUE), mais également du droit européen (accès au marché unique numérique de l'UE). Des clauses contractuelles types n'étant à elles seules pas suffisantes, il propose de supprimer cet alinéa, voire la seconde phrase, et la remplacer par un renvoi aux directives du PFPDT.

Al. 3

Alors que quelques participants[197] s'interrogent sur l'actualité de la « forme écrite », deux autres participants[198] saluent l'utilisation de cette forme pour l'autorisation de la délégation de deuxième rang. Ils relèvent toutefois que cette exigence ne figure pas dans la nLPD. Il se pose dès lors la question de savoir si cela peut réellement être imposé aux organes fédéraux qui ne sont pas soumis à la Directive 2016/680, l'art. 22, al. 2, Directive 2016/680 mentionnant le consentement par écrit dans le secteur public. Selon la suva, l'autorisation écrite des organes fédéraux correspond au standard du RGPD. Toutefois, l'art. 9, al. 3, nLPD ne

[194] Organisations : ASA, curafutura.

[195] Organisations : ASB, CFF, digitalswitzerland, economiesuisse, EXPERT suisse, H+, HKBB, HÄRTING, IGEM, la Poste, les banques domestiques, Migros, Raiffeisen, Ringier, Scienceindustries suisse, SDV, suva, Swissstaffing, thurbo, UTP, VUD, Walderwyss.

[196] Organisations : ASPS, ASSL, auto suisse, CURAVIVA Suisse, FSA, INSOS, IS, senesuisse, SPA, SPITEX suisse, Swiss Insights, UPSA, usam.

[197] Organisations : Creditreform, vsi.

[198] Organisations : HDC, swissprivacy.law.

prévoit pas de forme écrite. ASDPO est d'avis que l'accord écrit devrait également être appliqué au responsable privé. Curafutura ajoute que le numérique prenant de plus en plus de place, il serait opportun de proposer une alternative à la forme écrite. Il sied de s'inspirer de la nouvelle mouture de la loi fédérale sur le contrat d'assurance[199], entrée en force en janvier 2022. Celle-ci introduit la forme écrite ou « tout autre moyen permettant d'en établir la preuve par un texte ». Partant, des participants[200] proposent de reprendre cette dernière formule à l'image de l'art. 28, ch. 2, RGPD, qui par la locution « par écrit » couvre la forme électronique et tout autre forme permettant d'établir la preuve par texte. Au niveau rédactionnel, la proposition suivante est donnée : « par écrit ou sous forme électronique ou par toute autre forme permettant d'établir la preuve par texte ». BE estime que la forme écrite doit être remplacée par « toute autre forme de texte inaltérable ». En outre, le rapport explicatif doit préciser que la forme écrite désigne notamment les documents sur papier ou sous forme électronique. LU suggère qu'il pourrait être expressément mentionné la forme électronique : en utilisant des expressions telles que « consentement exprès », « établir sous forme de texte » ou « enregistrer ». La suppression des exigences de forme est de toute façon appropriée. Santésuisse relève que l'exigence de la forme écrite ne doit pas être un obstacle.

Curafutura est d'avis qu'une réserve permettant de s'opposer devrait remplacer l'approbation. BE propose qu'il soit précisé « qu'avec l'approbation préalable de l'organe fédéral ». Quelques participants[201] font remarquer qu'une autorisation générale conformément au RGPD est suffisante. Une autorisation écrite spécifique à chaque cas n'est, ainsi, pas nécessaire. Ils citent l'exemple des services en ligne standard, qui ne prévoient pas cette possibilité dans leurs conditions générales. Il ne serait donc plus possible d'obtenir de tels services.

VD relève une coquille : « Lorsque le responsable de traitement… » doit être corrigé par « Lorsque le responsable du traitement … ».

3.2.7 Art. 7 P-OLPD : Information du conseiller à la protection des données de l'organe fédéral

La disposition est jugée superflue. Sa suppression est demandée[202]. Quelques participants[203] rappellent que, conformément à l'art. 28 et à l'art. 10, al. 2, let. b, nLPD, le conseiller à la protection des données de l'organe fédéral collabore de toute façon à l'application des prescriptions en matière de protection des données. SO ajoute que la disposition ne tient pas suffisamment compte de cette exigence. Pour quelques participants[204], il semble contraire à l'approche fondée sur les risques de la nLPD que le conseiller à la protection des données ne soit informé qu'*a posteriori* de la conclusion d'un contrat d'externalisation ou lors d'un transfert de fonction. Les tâches du conseiller ou de la conseillère à la protection impliquent de telles transactions. Le rapport explicatif mentionne expressément les risques accrus liés au traitement des mandats. De surcroît, la participation à l'application des prescriptions relatives à la protection des données est l'une de ses tâches essentielles. Le conseiller à la protection

[199] LCA, RS **221.229.1**.

[200] Canton : LU ; organisations : ASSL, asut, auto suisse, CFF, Creditreform, Datenschutzguide.ch, DFS, H+, HDC, IGEM, la Poste, Migros, Ringier, SPA, Sunrise UPC, suva, SWICO, Swiss Insights, swissICT, thurbo, UTP, VUD, Walderwyss.

[201] Organisations : CFF, thurbo, UTP.

[202] Cantons : AG, GL, SH, SO, VD, ZH ; organisations : ASA, asut, curafutura, IGEM, privatim, santésuisse, Sunrise UPC, SWICO, swissICT, UTP. CFF, H+, la Poste, Migros, Ringier, suva, thurbo, UTP et Walderwyss demandent, à tout le mois, la suppression de la seconde phrase.

[203] Cantons : AG, BE, GL, NW, SH, SO, SZ, VD ; orgnisations : ATPrD, curafura, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim, santésuisse, suva.

[204] Cantons : AG, BE, GL, NW, SH, SZ, UR, VD, ZH ; organisations : ATPrD, Préposé à la protection des données de SZ, OW et NW, Préposé cantonal à la protection des données et à la transparence NE/JU, privatim.

des données doit être informé en temps utile, comme cela est prévu pour les projets des organes fédéraux pour le traitement automatisé des données personnelles (art. 31). La disposition doit, à tout le moins, être renforcée.

Quelques participants[205] sont d'avis que cette disposition empiète sur la liberté organisationnelle interne à l'entreprise. Une entreprise doit s'assurer que les contrats respectent les règles de protection des données. Ils demandent à ce que les entreprises de transport soient exclues du champ d'application de la disposition.

Deux participants[206] font remarquer que les organes fédéraux, comme les assurances maladie, ont d'innombrables contrats qui impliquent des traitements des données. L'approche basée sur les risques commande au conseiller ou à la conseillère à la protection des données de connaître les traitements particulièrement risqués au travers du registre des activités de traitement. Une obligation d'information supplémentaire, avec un tel degré d'absolu, n'est pas indispensable. Ce d'autant qu'il ne crée aucune valeur ajoutée pour les personnes concernées.

Le DFS souligne qu'à titre préventif les conseillers à la protection des données ont une grande importance. Cet aspect doit être pris en compte lors de l'élaboration de cet article, afin d'éviter autant que possible les problèmes ultérieurs. L'idée serait de mettre en place une consultation préalable du conseiller à la protection des données, ce qui implique également de siéger dans les organes correspondants.

HDC considère que l'obligation d'informer le conseiller à la protection des données peut avoir son intérêt. Il peine, toutefois, à saisir son rattachement avec la nLPD ainsi que les conséquences de sa violation. Il se demande si une des conséquences serait de rendre le traitement illicite et permettrait à la personne concernée de faire valoir des prétentions sur cette base (art. 41 nLPD). Des participants[207] rappellent que l'art. 29 nLPD prévoit déjà un devoir d'information qui est formulé de manière plus générale et qui englobe également les traitements sur mandat, pour autant que ceux-ci soient pertinents.

L'ASIP demande de préciser que « ne sont pas visés les organes fédéraux en tant que sous-traitants au sens de l'art. 2, al. 1, let. b, en relation avec l'art. 5, let. i, nLPD ».

Le swissICT ne comprend pas que des exigences particulières soient fixées au niveau de l'ordonnance, dès lors que l'art. 24 LPD règle la notification des violations de la sécurité des données. Les processus internes doivent pouvoir être réglés par l'organe fédéral lui-même. En outre, l'art. 29, al. 1, nLPD prévoit déjà un devoir d'information de l'organe fédéral envers le conseiller à la protection des données. Il souhaiterait des clarifications autour du terme « problème ».

3.2.8 Art. 8 P-OLPD : Evaluation du niveau de protection adéquat des données personnelles d'un Etat étranger ou d'un organisme international

VS salue l'élaboration d'une liste des États, secteurs et territoires avec un niveau de protection adéquat (annexe).

[205] Organisations : CFF, la Poste, thurbo, UTP.

[206] Organisations : ASA, curafutura.

[207] Organisations : asut, BNS, Sunrise UPC, suva, SWICO.

Quelques participants[208] appellent au respect du principe de la transparence, particulièrement en ce qui concerne les alinéas 3 à 5. Ce principe doit transparaître non seulement dans les résultats, mais également dans le processus de décision. Des participants[209] demandent que le libellé de la disposition précise qu'elle s'adresse de manière générale au Conseil fédéral. Divers participants[210] considèrent que la procédure d'évaluation doit être réglée, en particulier la procédure d'obtention de la décision d'adéquation, si celle-ci est sujette à recours ainsi que les cas d'exclusion. Les voies de droit doivent être ajoutées.

Le PPS s'inquiète que le transfert de l'évaluation de l'adéquation au Conseil fédéral (art. 16 nLPD) occasionne des décisions de nature politique et non pas basées sur une réelle expertise. Il propose, dès lors, que le PFPDT continue de procéder à l'évaluation. Quelques participants[211] demandent que soit ajouté dans la disposition que le niveau jugé adéquat est celui de la nLPD.

Selon GE, une liste non exhaustive des États dont la législation assure un niveau de protection adéquat n'est pas satisfaisante. Le maintien du système actuel, soit une liste exhaustive, doit être favorisé. Cette solution facilite l'application de la loi – tout particulièrement par les personnes et entreprises privées – et les échanges avec l'étranger.

Quelques participants[212] regrettent le défaut d'informations dans le rapport explicatif, notamment à qui s'adresse cette disposition et qui est tenu d'agir. Par ailleurs, comme cet article ne peut évidemment pas concerner le responsable privé, il convient de le préciser sans équivoque dans le texte de l'ordonnance.

Classtime estime que l'évaluation de l'adéquation doit être appréciée selon le contexte de l'utilisation des prestataires de services tiers étrangers. À titre 'illustratif, l'utilisation de produits Microsoft est très répandue, bien que Microsoft fasse largement appel à des prestataires de services tiers aux États-Unis (dépôts de fichiers et stockage en nuage). Les interdictions légales ne sont guère respectées par ce genre de multinationale. Partant, les petits fournisseurs suisses qui utilisent des prestataires de services tiers comme sous-traitants, notamment aux États-Unis, ne doivent pas être désavantagés. La transmission de données personnelles en vue de leur traitement par des prestataires de services tiers doit être considérablement assouplie afin d'être applicable *de facto* et évaluée selon la sensibilité des données. Notons en outre que des organes publics utilisent ces produits.

Al. 1

HDC reconnaît qu'une approche par catégories (un État, un territoire, un secteur déterminé) peut avoir son intérêt. Ce nonobstant, le siège de cette classification doit se trouver dans la loi. À défaut, il s'agit d'un procédé *ultra legem.* Par ailleurs, la notion de « secteur déterminé » n'est pas définie. Cela présente un risque pour son interprétation et son application. L'art. 16, al. 3, nLPD laisse au Conseil fédéral la possibilité de mettre en place des garanties à communiquer préalablement au PFPDT. Il ne s'agit pas d'une décision d'adéquation.

[208] Partis politiques : PPS, PVS.

[209] Partis politique : Le Centre ; organisations : AFPS, ASB, ASPS, Association de commerce, asut, CURAVIVA Suisse, DigiGes, digitalswitzerland, economiesuisse, EXPERTsuisse, HÄRTING, HKBB, INSOS, IS, la Poste, les banques domestiques, Raiffeisen, Scienceindustries suisse, SDV, senesuisse, SPA, SPITEX suisse, Stiftung für Konsumentenschutz, Sunrise UPC, SWICO, SwissHoldings, usam.

[210] Organisations : FRC, HDC, swissprivacy.law.

[211] Organisations : HDC, FRC.

[212] Organisations : Creditreform, vsi.

GL se félicite de l'ajout d'une distinction entre « État », « territoire » ou « secteur déterminé dans un État ». Celle-ci permet au Conseil fédéral de tenir compte des particularités légales et/ou locales dans sa décision d'adéquation. La FRC précise que la possibilité d'octroyer une autorisation lorsqu'un secteur déterminé d'un État accorde un niveau de protection suffisant doit être conditionnée au fait que le secteur déterminé n'est pas assujetti aux lois ou à certaines des lois de l'État dans lequel il se trouve. De même, seuls les territoires disposant d'une autonomie légale du point de vue de la protection des données devraient être éligibles. Les critères devraient figurer dans l'ordonnance. Selon swissprivacy.law, l'art. 8 diffère de l'art. 16 nLPD par l'ajout d'un territoire ou d'un secteur déterminé dans un État. Cette précision ne correspond pas à la volonté du législateur et doit être supprimée.

Selon divers participants[213], une seconde phrase doit être ajoutée à cet alinéa, notamment après l'énumération des critères (let. a à e). La formule serait la suivante : « Les responsables peuvent se fier à la décision du Conseil fédéral concernant le caractère adéquat de la protection des données conformément à la première phrase et ne doivent pas procéder à des clarifications supplémentaires ».

L'UBCS fait remarquer que la liste établie par le Conseil fédéral (art. 16, al. 1, nLPD) a un caractère contraignant pour tous les acteurs de l'adéquation. L'examen supplémentaire au cas par cas et l'évaluation qui en découle ne sont ni réalisables ni pertinents.

Al. 1 let. b

GL salue l'introduction du critère général du « respect des droits humains ».

Des participants[214] font remarquer que le respect des droits humains n'est pas un critère pertinent, notamment par son manque de clarté. Un tel critère n'a pas sa place lorsqu'il s'agit de déterminer si un État (ou un territoire ou un secteur spécifique) ou un organe international assure une protection adéquate des données. La protection des droits humains est, sans aucun doute, un aspect important auquel il sied de tenir compte de manière générale : par exemple, dans l'examen du respect des principes de protection de la protection de la personnalité, concernant les droits humains qui y sont liés. La notion de droits humains fait, indéniablement, référence aux droits fondamentaux inscrits dans la Constitution fédérale[215]. Ainsi l'adéquation ne dépend pas du fait qu'un État autoriserait la dissimulation du visage dans l'espace public ou ne garantirait pas la liberté de l'art ou le droit à un enseignement de base gratuit.

Al. 1 let. c

D'après swissICT, la prise en compte de la jurisprudence est trop contraignante et non adaptée à la pratique et nuit à la sécurité juridique. En effet, celle-ci conduirait à ce que l'évaluation doive être constamment révisée dès le prononcé d'une nouvelle décision concernant la protection des données. Il propose de remplacer le texte par : « la législation en vigueur en matière de protection des données ainsi que sa mise en œuvre et la jurisprudence pertinente ».

[213] Organisations : ASB, digitalswitzerland, economiesuisse, HKBB, la Poste, les banques domestiques, Raiffeisen, Scienceindustries suisse, SDV.

[214] Organisations : FRC, HDC, swissprivacy.law, UPSV.

[215] Cst. féd., RS **101**, art. 7 ss.

Al. 1 let. d

La FRC demande de préciser que la garantie d'un procès équitable est un critère important, afin d'assurer à la personne concernée dont les données pourraient être utilisées à l'étranger, une défense équitable.

Al. 1 let. e

Selon swissICT, la lettre devrait être supprimée. À tout le moins, la formulation doit s'inspirer des critères d'évaluation de la Commission européenne.

Al. 1 let. f

Selon Swimag, une lettre f doit être ajoutée à cet alinéa. En effet, la ou les personnes concernées par la communication de données personnelles à l'étranger ne doivent pas être privées de leurs droits. Elles ne doivent pas subir de désavantages par rapport à une non-communication, notamment entre le droit suisse et le droit étranger. Un examen minutieux et préalable des législations applicables est indispensable. Déterminer si un État, un territoire, un ou plusieurs secteurs déterminés dans un État ou un organe international garantit une protection adéquate des données ne sert pas à grand-chose sans les critères ajoutés figurant dans cet examen de droit comparé.

Al. 1 let. g

Swimag demande, en outre, que soit ajouté que dans tous les cas de communication de données personnelles à l'étranger, le consentement écrit de la ou des personnes concernées est requis.

Al. 3

Quelques participants[216] rappellent que le PFPDT informait régulièrement sur son site Internet des développements et adaptations actuels. Le Conseil fédéral devrait rendre ses décisions accessibles au public de manière transparente. Il est proposé de compléter l'alinéa de la manière suivante : « Les décisions, modifications et adaptations doivent être motivées et rendues accessibles au public sans délai et de manière complète ».

Quelques participants[217] sont d'avis que les intervalles entre les évaluations doivent être indiqués de manière plus précise. Il sied d'ajouter qu'elles « sont périodiquement, mais au moins une fois par an ».

SPA propose d'ajouter dans le texte que l'obligation de réévaluer incombe au Conseil fédéral.

Al. 4

À l'instar de l'art. 16, al. 2, nLPD, l'art. 8, al. 4, se réfère à la notion de décision. Selon le TAF, se pose alors la question de savoir s'il s'agit d'une décision au sens de l'art. 5 loi fédérale sur la procédure administrative[218].

[216] Orgnisation : DigiGes ; parti politique : PVS. Dans le même sens: Stiftung für Konsumentenschutz

[217] Organisations : ASDPO, ASPS, CURAVIVA suisse, INSOS, IS, senesuisse, SPITEX suisse.

[218] PA, RS **172.021**.

L'ASDPO souhaite que la procédure soit éclaircie, notamment si des recours sont possibles. En effet, indiquer que la nouvelle décision n'a pas d'effet sur les données déjà transférées à l'étranger est erroné. Les données déjà transférées sous un régime d'adéquation sont traitées dans un État qui n'offre (peut-être) plus de niveau de protection adéquat, ce qui peut porter atteinte aux droits de la personnalité des personnes concernées. À tout le moins, il est demandé de supprimer la seconde phrase.

SwissICT se demande ce qu'il est entendu par une « communication des données déjà effectuée ». Cet alinéa est-il applicable si une protection des données appropriée est garantie ? Il considère que pour les responsables, cette disposition aurait dû figurer au niveau de la loi. Swimag considère que cette nouvelle décision n'a aucune incidence sur les communications de données déjà effectuées. Elle est applicable, dans la mesure du possible, aux communications de données déjà effectuées. Il convient d'éviter, de compenser ou de réparer les dommages ou les violations passés et ultérieurs.

Al. 5

Le PVS précise que le PFPDT n'est pas seulement consulté, mais que ses avis doivent également être pris en compte matériellement dans l'évaluation. L'alinéa doit être adapté en ce sens.

La FER est d'avis que l'usage d'une liste « positive » crée une insécurité juridique. Dans cet ordre d'idées, si un État n'y figure pas, cela peut signifier qu'il n'ait simplement pas encore fait l'objet d'un examen de la part du Conseil fédéral. La pratique actuelle doit être maintenue. Ainsi le PFPDT publie un document dans lequel il précise à côté de chaque Etat si celui-ci atteint un niveau adéquat pour les personnes

Al. 6

Certains participants[219] proposent la formule rédactionnelle suivante : « Le Conseil fédéral consulte le PFPDT avant toute décision relative à l'adéquation de la protection des données ». Afin que la décision du Conseil fédéral ne soit pas politique, le PFPDT doit être réellement consulté[220] ou même disposer d'un droit de veto[221]. Des participants[222] relèvent que le PFPDT doit être formellement consulté. Les appréciations d'organisations internationales ou d'autorités étrangères peuvent être (matériellement) prises en compte. Il est demandé que soit formulé explicitement, au moins dans le rapport explicatif, que les avis du PFPDT doivent également être pris en compte sur le plan matériel.

Al. 7

Pour plus de clarté, un petit nombre de participants[223] proposent l'ajout d'un alinéa 7 dont le contenu serait le suivant : « Si des données personnelles sont communiquées à l'étranger dans un État ou un territoire ne disposant pas d'une protection des données adéquate, des mesures complémentaires aux garanties prévues à l'art. 16, al. 2, let. b et c, LPD peuvent

[219] Organisations : ASB, digitalswitzerland, economiesuisse, HKBB, la Poste, les banques domestiques, Raiffeisen, Scienceindustries suisse, SDV, SPA, Stiftung für Konsumentenschutz.

[220] Organisations : DigiGes, Stiftung für Konsumentenschutz.

[221] Organisation : Stiftung für Konsumentenschutz.

[222] Cantons : AG, BE, GL, NW, SH, SZ, VD, ZH ; organisations : ATPrD, OW et NW, privatim, Préposé cantonal à la protection des données et à la transparence NE/JU, Préposé à la protection des données de SZ.

[223] Organisations : ASB, digitalswitzerland, economiesuisse, HKBB, la Poste, les banques domestiques, Raiffeisen, Scienceindustries suisse, SDV.

être nécessaires pour assurer une protection des données appropriée. Le Conseil fédéral détermine si des mesures complémentaires sont nécessaires. Les États et territoires concernés sont énumérés à l'annexe 1a. La décision du Conseil fédéral concernant la nécessité de mesures complémentaires est contraignante ».

3.2.9 Art. 9 P-OLPD : Clauses de protection des données d'un contrat et garanties spécifiques

Quelques participants[224] soutiennent la volonté du Conseil fédéral d'introduire certaines exigences minimales et des garanties spécifiques ; ce d'autant que les clauses ou garanties (art. 16, al. 2, let. b, nLPD) sont uniquement portées à la connaissance du PFPDT.

Des critiques s'élèvent, toutefois, autour des exigences introduites par cette disposition. Le niveau de détail est jugé inutile[225].

HÄRTING regrette que les exigences de cet article ne s'orientent pas plus sur les rôles d'exportateur (responsable du traitement) et d'importateur (destinataire).

Al. 1

La FSA est d'avis que l'énumération est une liste exemplative. Dans la négative, il conviendrait de préciser qu'une distinction doit être faite entre les contrats dans lesquels le destinataire est un responsable du traitement et ceux dans lesquels il agit en tant que sous-traitant.

Quelques participants[226] sont d'avis que, bien que cohérentes avec l'objectif de protection des données, ces exigences entraînent des coûts de traitement élevés pour les entreprises impliquées. Elles doivent être réduites au minimum, voire les lettres b, c, g, h et i doivent être supprimées.

Des participants[227] sont d'avis que l'énumération des exigences d'un « Data Transfer Agreement » est inadaptée et doit être supprimée. À ce sujet, il importe de préciser que le PFPDT doit de toute façon les vérifier. Cette énumération ne fait, toutefois, pas de distinction entre le type de transfert ou les rôles de l'exportateur et de l'importateur. Or ces derniers sont déterminants pour le contenu du contrat, comme le montrent par exemple les clauses contractuelles types de la Commission européenne (EU SCC). Il sied de relever que ces clauses sont désormais reconnues par le PFPDT. Partant, il ne fait pas sens d'imposer des obligations au sous-traitant par contrat, alors que celles-ci ne reposent pas sur la nLPD. Le RGPD fournit une protection adéquate. Celle-ci est tout aussi bonne pour les données communiquées par les responsables suisses. À tout le moins, il se justifie de modifier le catalogue d'exigences pour couvrir différentes constellations (responsable du traitement, sous-traitant), voire remplacer le « au moins » par « selon les circonstances ». Finalement et dans la mesure où les personnes concernées doivent être informées, il manque des règles sur la notification des violations de la sécurité des données. D'autres participants[228] se posent également la question de la base légale. Ils précisent que les critères ne doivent pas être soumis

[224] Parti politique : PS ; organisation : USS.

[225] Organisations : CURAVIVA suisse, EXPERTsuisse, SPITEX suisse, usam.

[226] Organisations : ASPS, CURAVIVA suisse, digitalswitzerland, economiesuisse, EXPERTsuisse, HKBB, INSOS, IS, les banques domestiques, Raiffeisen, Scienceindustries suisse, SDV, senesuisse, SPITEX suisse.

[227] Organisations : ASB, asut, CFF, DFS, digitalswitzerland, economiesuisse, H+, HKBB, IGEM, la Poste, les banques domestiques, Migros, Raiffeisen, Ringier, Scienceindustries suisse, SDV, SPA, Sunrise UPC, suva, SWICO, thurbo, UTP, VUD, Walderwyss.

[228] Organisations : Creditreform, Datenschutzguide.ch, vsi.

cumulativement à tous les systèmes juridiques possibles, ce qui serait délicat pour le responsable du traitement.

L'ASDPO relève qu'il manque un point sur le droit d'audit de l'exportateur des données vis-à-vis de l'importateur. Il propose, dès lors, d'ajouter une lettre m sur le droit d'audit et une lettre n sur l'annonce des violations de la sécurité des données.

La Poste est d'avis que les lettres d, e, f et j doivent être supprimées.

Quelques participants[229] relèvent l'absence de distinction entre les rôles d'exportateur et d'importateur. Ils se demandent s'il ne serait pas plus pratique de remplacer entièrement le texte de l'art. 9 et l'aligner sur l'art. 28, ch. 4, RGPD, dès lors qu'en pratique il sied déjà de s'y conformer.

D'après Bär & Karrer, les lettres a à k définissent le contenu minimal des clauses de protection des données. Le RGPD ne connaît pas de telles énumérations (art. 43, ch. 3, RGPD). Seul le contenu minimum des règles internes contraignantes en matière de protection des données est réglementé. Pour Walderwyss, il manque notamment les accords sur la manière dont les législations locales sont examinées ou prises en compte et la procédure à suivre en cas d'accès par les autorités.

Al. 1 let. a

Des participants[230] font remarquer que le principe de transparence fait défaut. Il devrait être ajouté au texte.

Al. 1 let. d et e

De l'avis de quelques participants[231], mentionner le nom des États ou des organisations internationales auxquels les données personnelles sont communiquées ne s'appuie sur aucune base légale en cas de retransmission. La question de la retransmission nécessite des éclaircissements. Ce nonobstant, il suffit de désigner le destinataire. Les clauses contractuelles types de la Commission européenne se limitent également à cela. SwissICT considère qu'il manque une base légale pour exiger que les pays ou les organisations vers lesquels les données sont transférées soient mentionnés. Par conséquent, il demande la suppression de ces lettres.

Al. 1 let. f

Divers participants[232] ne voient pas l'intérêt de cette lettre. Elle serait une redondance couverte par le principe de la proportionnalité. La Poste estime, en outre, qu'elle n'a pas de base légale.

[229] Organisations : Bär & Karrer, swissICT.

[230] Organisations : ASDPO, CFF, digitalswitzerland, economiesuisse, H+, HKBB, la Poste, les banques domestiques, Raiffeisen, Ringier, Scienceindustries suisse, SDV, SPA, suva, thurbo, UTP, VUD, Walderwyss.

[231] Organisations : CFF, digitalswitzerland, economiesuisse, H+, HKBB, la Poste, les banques domestiques, Raiffeisen, Ringier, Scienceindustries suisse, SDV, SPA, suva, thurbo, UTP, VUD, Walderwyss.

[232] Organisations : CFF, digitalswitzerland, economiesuisse, H+, HKBB, la Poste, les banques domestiques, Raiffeisen, Ringier, Scienceindustries suisse, SDV, SPA, suva, swissICT, thurbo, UTP, VUD, Walderwyss.

Al. 1 let. g

Quelques participants[233] considèrent que l'expression « habilités à traiter les données » est inadaptée, voire superflue. À leur sens, seuls les « destinataires » sont importants, c'est-à-dire les parties qui concluent le contrat. SwissICT propose la suppression de la lettre.

Al. 1 let. h

Plusieurs participants[234] sont d'avis que les mesures garantissant la sécurité des données personnelles figurent déjà dans la clause de protection des données ou dans les garanties spécifiques elles-mêmes, conformément à l'art. 9, al. 2. Partant, l'obligation renouvelée du responsable de prendre des mesures appropriées pour garantir le respect des clauses de protection des données est redondante. Il faudrait plutôt y parvenir en obligeant par écrit le destinataire à respecter ou à observer les clauses de protection des données. Ces participants ne voient pas l'utilité de cette lettre et la trouve disproportionnée. La disposition doit être supprimée.

L'ASDPO propose la formule suivante : « les mesures techniques et organisationnelles ».

Al. 1 let. j

Deux participants[235] considèrent qu'il n'appartient pas au sous-traitant d'informer les personnes concernées. Ils demandent l'introduction parmi les clauses de protection d'une obligation pour les destinataires d'informer les personnes concernées. À l'inverse, BE est d'avis que cette lettre doit être supprimée. Conformément aux art. 19 à 23 nLPD, l'obligation d'informer n'incombe qu'aux autorités responsables. Une extension de l'obligation au destinataire des données semble peu judicieuse et n'est probablement pas faisable.

Certains participants[236] estiment que l'obligation nouvelle doit figurer dans une base légale au sens formelle. Suisa est d'avis que cette lettre contredit l'art. 19, al. 4, et l'art. 25, al. 1, nLPD. Ces deux dernières dispositions légales définissent de manière exhaustive l'étendue de l'obligation d'informer et de renseigner. De plus, cette lettre est souvent inapplicable d'un point de vue purement pratique. Le destinataire des données à l'étranger ne connaît pas les personnes concernées et leurs adresses pour les informer. La suppression de cette lettre est demandée.

Santésuisse juge cette lettre peu précise et s'interroge sur les raisons qui obligeraient le destinataire à informer les personnes concernées. Cela devrait rester de la compétence du responsable du traitement, ne s'agissant pas d'une sous-traitance au sens de l'art. 9 nLPD. En outre, force est de constater qu'il n'est pas expliqué ce que signifie « informer du traitement ». SwissICT propose la suppression de cette lettre. Il renvoie à ce sujet à la remarque de l'art. 9, al. 1, relative à l'absence de distinction selon les rôles des parties.

[233] Organisations : CFF, digitalswitzerland, economiesuisse, H+, HKBB, la Poste, les banques domestiques, Raiffeisen, Ringier, Scienceindustries suisse, SDV, SPA, suva, swissICT, thurbo, UTP, VUD, Walderwyss.

[234] Organisations : Digitalswitzerland, economiesuisse, HKBB, Hotelleriesuisse, les banques domestiques, Raiffeisen, Scienceindustries suisse, SDV, usam.

[235] Organisations : ASA, curafutura.

[236] Organisations : Suisa, Walderwyss.

HÄRTING relève qu'il convient de se référer à lettre i, s'il s'agit d'un « transfert à terme ». La question peut être laissée ouverte de savoir si l'obligation d'information doit être imposée à l'exportateur ou à l'importateur.

Al. 1 let. k

Suisa estime que l'obligation nouvelle doit figurer dans une base légale au sens formel. Il est d'avis que le chiffre 1 contredit l'art. 19, al. 4, et l'art. 25, al. 1, nLPD. Ces deux dernières dispositions légales définissent de manière exhaustive l'étendue de l'obligation d'informer et de renseigner. De surcroît, cette disposition conduirait à une application extraterritoriale du droit suisse, ce qui est contraire au droit international et donc impossible à mettre en œuvre. Il demande la suppression de cette lettre.

SwissICT demande la suppression de cette lettre. En cas de communication dans le cadre d'un traitement de commande, cela n'est pas légitime. Il est renvoyé à la remarque générale de l'art. 9, al.1. Il propose, en outre, d'ajouter un renvoi entre parenthèses vers la disposition de la LPD où ce droit de la personne concernée est réglé.

Selon HÄRTING, la nLPD ne connaît comme droit d'opposition que le droit de la personne concernée de s'opposer à la communication de données personnelles par l'organe fédéral responsable (art. 37 nLPD). L'art. 9, al. 1, let. k, ne fait probablement pas référence à ce droit. Le rapport explicatif désigne ici « le droit de s'opposer au traitement de données personnelles ». Il n'apparaît pas clairement à quel droit des personnes concernées de la nLPD il est fait référence ; probablement le droit de la personne concernée de révoquer à tout moment le consentement qu'elle a donné, raison pour laquelle la let. k doit être adaptée dans ce sens.

L'ASDPO propose d'ajouter le droit à la remise des données (art. 28 et 29 nLPD).

Swimag propose l'ajout d'un chiffre 5 avec la formule rédactionnelle suivante : « de ne pas consentir au traitement des données ».

Al. 2

CFC souhaite des exemples de « mesures appropriées ». Cela permettrait une meilleure appréhension de la situation par le responsable du traitement, voire la personne concernée.

Pour certains participants[237], le verbe « s'assurer » est quelque peu excessif. Quelques-uns expliquent que ce verbe implique une garantie du respect des clauses ou une responsabilité causale, pour laquelle il n'existe aucune base légale. Ainsi dite obligation ne peut raisonnablement être exigée. Ils proposent de favoriser la formule suivante : « veiller à » ou « veiller de manière raisonnable ». De plus, des participants[238] relèvent que cet alinéa est trop vague. Il se pose la question de savoir ce que pourraient être ces mesures ; d'autant que le RGPD ne connaît pas une telle réglementation. Cet alinéa doit être supprimé.

Divers participants[239] soulignent que les clauses de protection devraient contenir l'obligation pour le destinataire d'informer les personnes concernées. Il n'appartient pas au sous-traitant d'informer les personnes concernées. Cette tâche incombe au responsable du traitement.

[237] Organisations : ASP, Association de commerce, Creditreform, curafutura, economiesuisse, EPS, FSA, FSEP, HotellerieSuisse, IGEM, SPA, suva, Swissstaffing, usam, vsi.

[238] Organisations : asut, Sunrise UPC, SWICO, swissICT.

[239] Organisations : digitalswitzerland, economiesuisse, HKBB, les banques domestiques, Raiffeisen, Scienceindustries suisse, SDV.

Al. 3

Quelques participants[240] considèrent que selon l'art. 16, al. 2, let. b et c, nLPD les clauses de protection des données et les garanties spécifiques doivent être communiquées préalablement au PFPDT. Ils demandent que la phrase introductive de l'art. 9, al. 3 soit révisée, voire tout l'alinéa adapté. En effet, l'alinéa suggère qu'il pourrait y avoir une situation dans laquelle la non-communication conduirait à une communication à l'étranger conforme au droit. SH insiste sur le fait que cet alinéa ne doit pas affaiblir l'art. 16, al. 2, let. b et c nLPD. Selon VD, il convient de souligner que dans le contexte du RGPD et des traitements et transferts entre personnes morales d'une même entité ou appartenant au même groupe ces dernières doivent être considérées comme tierces parties. Dès lors, un contrat de sous-traitance et des clauses de protection sont exigés. UPSV estime que la non-approbation des garanties spécifiques de protection des données par le PFPDT (mais simple transmission avant la communication des données à l'étranger) crée un risque non négligeable que l'évaluation des risques par les responsables du traitement et les sous-traitants soit différente, tant dans le secteur privé que dans le secteur public. Il est demandé que cette simple information soit remplacée par une obligation d'approbation du PFPDT.

3.2.10 Art. 10 P-OLPD : Clauses types de protection des données

Des participants[241] saluent cette disposition, et notamment le fait que le PFPDT publie une liste des clauses types de protection des données. En outre, CFC souhaite des exemples de critères permettant d'apprécier si les mesures sont appropriées.

De manière générale, la suppression de la disposition est demandée, voire son adaptation[242]. Au vu de l'introduction des clauses types de protection des données, la disposition est jugée excessive[243], et même superflue[244]. Elle est jugée trop vague, n'étant pas précisé ce que pourraient être ces mesures[245]. Des précisions sont nécessaires. Le rapport explicatif doit mentionner que les destinataires ne sont pas obligés de respecter la législation suisse en matière de protection des données (art. 6, al. 2, nLPD)[246].

Le TAF s'interroge sur la « forme juridique » des clauses types de protection des données publiées par le PFPDT. Il est d'avis qu'il ne peut s'agir d'une décision susceptible de recours au sens de l'art. 5, al. 1, PA ; en particulier lorsque le PFPDT les établit, d'office, en l'absence de toute requête expresse d'un administré. Il relève que la publication de clauses types ne crée, ne modifie ou n'annule pas des droits et obligations pour un particulier et ne vise pas à s'appliquer à un cas d'espèce. À son sens, elles prennent la forme d'une recommandation générale et abstraite. La vérification de la conformité de la communication avec les règles sur la protection des données devrait s'effectuer *ex post*, dans le cadre d'une enquête menée par

[240] Cantons : AG, BE, GL, NW, SZ., VD ; organisations : ATPrD, OW et NW, privatim, Préposé cantonal à la protection des données et à la transparence NE/JU, Préposé à la protection des données de SZ.

[241] Organisations : ASPS, CURAVIVA, INSOS, IS, senesuisse, SPITEXsuisse.

[242] Organisation : ASB, ASP, ASSL, Association de commerce, asut, auto suisse, CFC, CFF, Creditreform, EPS, FER, FSA, FSEP, H+, HÄRTING, HotellerieSuisse, IGEM, la Poste, les banques domestiques, Migros, Raiffeisen, Ringier, santésuisse, SPA, Sunrise UPC, suva, SWICO, Swiss Insights, swissICT, TAF, thurbo, UPSA, UTP, vsi, VUD, Walderwyss.

[243] Organisations : HotellerieSuisse, vsi.

[244] Organisations : asut, HotellerieSuisse, Sunrise UPC, SWICO, swissICT, Walderwyss.

[245] Organisations : asut, digitalswitzerland, economiesuisse, HKBB, les banques domestiques, Raiffeisen, Scienceindustries suisse, SDV, Sunrise UPC, SWICO, swissICT.

[246] Organisations : auto suisse, digitalswitzerland, economiesuisse, HKBB, les banques domestiques, Raiffeisen, Scienceindustries suisse, SDV, Swiss Insights.

le PFPDT et qui aboutirait, là et là seulement, à une décision susceptible de recours (art. 52 nLPD).

Al. 1

À l'instar des précédentes dispositions, il est souhaité que le responsable du traitement « veille à ce » que le destinataire respecte les clauses types de protection des données, au lieu d'un devoir de « s'en assurer », notamment par le biais d'un audit[247]. Santésuisse considère que cette obligation est impossible à mettre en œuvre au regard des dispositions pénales. Quelques participants[248] expliquent que cet alinéa entraîne une responsabilité causale et serait impossible à respecter. À tout le moins, le responsable doit prendre des mesures appropriées pour contribuer à ce que le destinataire les respecte.

La suva déclare que les mesures sont appropriées lorsqu'elles correspondent à l'état de la technique ainsi qu'aux circonstances concrètes. Les clauses types actuelles, qui sont largement utilisées dans la pratique, exigent de toute façon des obligations de diligence correspondantes de la part de l'exportateur.

Auto suisse précise que l'adéquation des mesures exigées dépend des circonstances dans le cas concret et que les exigences sont plus élevées, notamment lorsqu'il s'agit de données personnelles sensibles.

Al. 2

Certains participants[249] soutiennent la publication par le PFPDT d'une liste de clauses types de protection des données.

3.2.11 Art. 11 P-OLPD : Règles d'entreprise contraignantes

Al. 1

Deux participants souhaitent que l'on précise à partir quel moment des entreprises sont considérées comme faisant partie d'un même groupe[250]. L'ASDPO se demande s'il est nécessaire que les entreprises d'un groupe soient détenues à plus de 50 % par les mêmes actionnaires et ce qu'il en est des succursales. HÄRTING explique qu'on parle en règle général d'entreprises affiliées lorsqu'une société détenant la majorité du capital ou des voix regroupe une ou plusieurs sociétés sous une direction unique.

Classtime relève que les Binding Corporate Rules (BCR)[251] devraient également s'appliquer à tous les prestataires de services dans un rapport contractuel direct[252].

[247] Organisations : ASB, ASP, Association de commerce, auto suisse, EPS, FSA, FSEP, HotellerieSuisse, HÄRTING, IGEM, la Poste, les banques domestiques, Raiffeisen, SPA, suva, Swiss Insights, swissICT, Swissstaffing, usam, vsi, Walderwyss.

[248] Organisations : ASB, la Poste, les banques domestiques, suva, swissICT.

[249] Organisations : ASPS, CURAVIVA suisse, INSOS, IS, senesuisse, SPITEX suisse.

[250] Organisations : ASDPO, HÄRTING.

[251] Les règles d'entreprise contraignantes (Binding Corporate Rules - BCR) sont des directives relatives à la protection des données auxquelles les entreprises établies dans l'UE doivent se soumettre pour transmettre des données à caractère personnel à des pays situés hors de l'UE à d'autres entreprises qui font partie du même groupe. Ces règles doivent contenir tous les principes généraux de protection des données et les droits applicables pour assurer la garantie nécessaire en matière de transmission de données. Elles doivent être juridiquement contraignantes et appliquées par toutes les entités concernées du groupe d'entreprises.

[252] P. ex. conseillers, freelance, développeurs, agences.

Al. 2

Selon EXPERTsuisse, l'art. 11 P-OLPD ne va pas aussi loin que l'art. 47 RGPD : les BCR actuelles sont souvent formulées de façon à être conformes au droit européen. La FER note en revanche que les exigences posées à cet alinéa dépassent le cadre de l'art. 16, al. 2, let. e, nLPD et que la let. a reprend le RGPD; ce qui n'est pas nécessaire. Il suffirait de conserver la lettre b de cet alinéa.

Elle estime également que l'art. 6, al. 5, OLPD en vigueur prévoit que le préposé examine les garanties et les règles de protection des données qui lui sont annoncées et communique son résultat au maître du fichier dans les 30 jours, mais ne l'oblige pas à partager les informations requises par l'art. 11, al. 2, let. a, P-OLPD. Dans cette optique, elle réclame que l'art. 11 P-OLPD fixe un délai au PFPDT pour communiquer son résultat. D'après elle, il faut conserver le délai de 30 jours fixé à l'art. 6, al. 5, OLPD actuelle.

3.2.12 Art. 12 P-OLPD : Codes de conduite et certifications

Al. 2

Un petit nombre de participants sont d'avis que le code de conduite ne peut pas contenir les points mentionnés à l'art. 9, al. 1, P-OLPD car, de par sa nature, il est abstrait et n'est pas formulé pour des entreprises spécifiques. D'après eux, il ne faudrait dans l'idéal que la finalité des points visés à l'art. 9, al. 1, P-OLPD[253].

L'UPSV estime que le code de conduite et les certifications devraient être approuvés par le PFPDT alors même que l'art. 9 P-OLPD, auquel il est fait référence, ne prévoit qu'une annonce au PFPDT, et pas son approbation. Il est difficile de savoir quand informer le PFPDT suffit et quand son approbation est nécessaire. Une harmonisation est souhaitée. L'ASDPO aimerait quant à elle supprimer l'approbation du PFPDT[254]. USS et PS sont en revanche favorables à l'obligation de disposer de son approbation. Classtime demande que des degrés de sensibilité soient introduits dans le contexte de l'application de l'art. 12 P-OLPD afin de satisfaire au principe de la proportionnalité.

Enfin, VUD préfèrerait, pour la version linguistique allemande, que l'on utilise à l'alinéa 2 les termes de « *Regelungen* » ou « *Punkten* » en lieu et place d'« *Angaben* ».

Al. 3

Le canton de Soleure fait remarquer qu'il faut préciser le caractère de l'engagement « exécutoire » car bien que des obligations légales puissent théoriquement être mises en œuvre dans certains États, en pratique, cela n'est pas possible. Il est important que l'applicabilité ne demande pas des efforts disproportionnés.

Certains participants à la procédure considèrent qu'il est difficile de savoir si les conditions découlant de l'art. 12, al. 2 et 3 P-OLPD ne restreindraient pas trop le champ d'application des codes de conduite et des certifications. Il est en revanche nécessaire de veiller à l'impact

[253] Organisations : IGEM, suva, VUD.

[254] Implicitement aussi l'organisation Classtime.

global des instruments et éventuellement de les soumettre à la bénédiction du PFPDT. Il faudrait donc faire une exception, et dire que les al. 2 et 3 ne sont pas applicables si le PFPDT a approuvé le code de conduite ou la certification[255].

Rapport explicatif

Le canton de Soleure estime que le rapport explicatif devrait clairement faire apparaître le fait que les codes de conduite peuvent uniquement provenir des associations professionnelles et économiques et non pas des responsables du traitement individuels.

3.2.13 Art. 13 P-OLPD : Modalités du devoir d'informer

Al. 1

Deux participants approuvent expressément cette disposition. Elle est à leurs yeux essentielle pour le droit à l'autodétermination des individus concernés qui pourront ainsi exercer leurs droits[256]. Des participants issus d'horizons variés veulent que le sous-traitant soit supprimé de cet article, et de manière générale du P-OLPD, parce que son devoir d'informer n'est pas applicable en pratique et inutile[257]. Il n'existe pas de base légale pour fixer de telles obligations. En outre, la nLPD ne prévoit pas de responsabilité du sous-traitant[258]. Les autorités cantonales de protection des données des cantons de Neuchâtel et du Jura reprochent elles aussi à la formulation de l'art. 13, al. 1, P-OLPD de ne pas respecter la hiérarchie des normes. En effet, elle est très extensive par rapport au texte de la nLPD, d'autant plus que la distinction entre le responsable du traitement et le sous-traitant est parfaitement respectée dans les autres dispositions de la nLPD. Bien que le titre du chapitre 3 nLPD mentionne les « Obligations du responsable du traitement et du sous-traitant », il est douteux que le législateur ait voulu imposer les mêmes obligations aux sous-traitants et aux responsables du traitement. Ce titre serait a priori dû à l'obligation imposée aux sous-traitants à l'art. 24, al. 3, nLPD.

En outre, une responsabilité du sous-traitant est contraire à la logique de la nLPD[259]. Les sous-traitants exécutent uniquement leurs tâches en fonction des instructions et des objectifs énoncés par le responsable du traitement. Selon les art. 19 ss nLPD, le devoir d'informer revient exclusivement aux responsables du traitement mais pas aux sous-traitants, qui doivent uniquement se tenir aux obligations contractuelles ou aux dispositions légales[260]. De facto, la relation contractuelle conclue pour le mandat prendrait fait ou serait tout du moins fortement touchée. Le responsable perdrait sa fonction de chef d'entreprise et, à cet égard, son obligation de surveillance vis-à-vis du sous-traitant[261]. Le cas échéant, l'accomplissement de l'obligation pourrait passer par une délégation contractuelle, mais les soumettre tous les deux à

[255] Organisations : Creditreform, usam, vsi.

[256] Organisations : DigiGes, FRC.

[257] Cantons : BE; partis : Le Centre; organisations : ASA, ASSL, BNS, curafutura, EXPERTsuisse, SSMD, UPSA.

[258] Cantons : BE, LU, ZH; partis : Le Centre, PLR ; organisations : ASA, ASB, auto suisse, BNS, Coop, curafutura, Datenschutzguide.ch, DFS, economiesuisse, FSA, HÄRTING, HotellerieSuisse, IGEM, proFonds, santésuisse, SDV, SPA, SSMD, suva, SWICO, swissICT, swissstaffing, UBCS, UVS, VUD, Walderwyss.

[259] Et par ailleurs la logique du RGPD. Organisations : Association de commerce, Econmiesuisse, FMH, FSA, la Poste, Migros, Raiffeisen, Scienceindustries suisse, SwissHoldings, UBCS, UVS.

[260] Cantons : BE, LU, ZH, partis : Le Centre, PLR, organisations : ASA, ASB, ASDPO, Association de commerce, curafutura, economiesuisse, EXPERTsuisse, FMH, FSA, la Poste, Migros, proFonds, Raiffeisen, Scienceindustries suisse, SWICO, UVS, vsi, VUD.

[261] Organisations : ASB, la Poste.

l'obligation d'informer est contraire à la logique du système. C'est pourquoi il est tout au plus possible de remplacer le « et » par un « ou » [262].

D'après l'AFBS, si le sous-traitant avait la responsabilité, il y aurait un risque que l'information soit communiquée plusieurs fois à la personne concernée, ce qui pourrait entraîner des contradictions. Le sous-traitant ne dispose souvent pas de l'information nécessaire ou ne sait pas clairement quelles informations peuvent et doivent être données à qui[263]. En outre, une violation de cette obligation serait passible d'une sanction au sens de l'art. 60 nLPD, ce qui implique que l'on introduirait aussi par ce biais une responsabilité pénale du sous-traitant et des personnes qui agissent pour lui[264].

Les autorités cantonales de protection des données du canton de Neuchâtel et du Jura signalent que cette norme n'est pas simple d'application parce qu'elle impliquerait la mise en place d'une règle de coordination. Qui devrait être poursuivi pour la violation de l'art. 60 nLPD ? Le canton de Vaud estime que la coordination entre responsable du traitement et sous-traitant devrait être clairement réglée. Le canton de Schwyz critique quant à lui le manque de clarté de la disposition qui implique que les responsables et les sous-traitants devraient s'informer mutuellement[265]. SWICO ajoute que l'al. 1 et les explications ne sont dans l'ensemble pas précises, ce qui serait source d'insécurité juridique. Dans l'intérêt de la sécurité juridique, Curafutura trouve que l'on devrait clarifier la manière dont devoir d'informer pourrait être rempli[266].

Pour certains, instaurer la responsabilité des sous-traitants serait un Swiss Finish[267]. En effet, d'après ASB, cela compliquerait l'échange transfrontières de données par rapport à l'UE, ce qui entrerait en contradiction avec l'une des raisons principales ayant motivé la révision de la législation suisse sur la protection des données.

Outre la question des obligations du sous-traitant, d'autres aspects ont également fait l'objet de critiques. La VUD remarque que l'art. 19 nLPD prévoit un devoir d'informer les personnes concernées. Le fait de rendre les données accessibles suffit. Il ne faut pas que le choix du verbe « *mitteilen* » (communiquer) soit assimilé à un durcissement de la disposition, c'est pourquoi un verbe tel que « *zur Verfügung stellen »* (mettre à disposition) serait plus adapté. Il exprime mieux le fait que les personnes concernées ont une certaine obligation de collaborer[268] et correspond à l'objectif du RGPD[269].

PVS et DigiGes souhaitent que l'adjectif « transparente » soit ajouté à l'énumération concernant la forme du renseignement, parce qu'il figure dans le RGPD[270]. Walderwyss estime quant à lui que la précision « de manière concise, compréhensible et facilement accessible » est superflue au vu de l'exigence de transparence.

[262] Organisations : Association de commerce, Creditreform, vsi.

[263] Et organisation: Economiesuisse.

[264] Organisations : Economiesuisse, SwissHoldings.

[265] Cantons : SZ; organisation : UVS.

[266] Et organisations : ASA, ProFonds.

[267] Parti : PLR; organisations : ASB, Digitalswitzerland, economiesuisse, SwissHoldings, UBCS.

[268] Organisations : BNS, Economiesuisse, EXPERTsuisse, IGEM, SPA.

[269] Organisations : SPA, suva, swissICT, Walderwyss.

[270] Parti : PVS; organisation : DiGes.

Un autre thème important est celui du « premier niveau de communication ». Contrairement à ce qui figure dans le rapport explicatif, des participants demandent que l'information ne doive pas obligatoirement être transmise dans le premier niveau de communication. Certains d'entre eux considèrent que les explications du rapport sont purement et simplement fausses. Ils déplorent l'absence de base légale appropriée[271]. L'art. 19, al. 1, nLPD prescrit que le responsable du traitement informe la personne concernée « de manière adéquate » de la collecte de données personnelles. La question de savoir si une communication est « adéquate » dépend toutefois des circonstances du cas précis[272]. Le commentaire de l'art. 13, al. 1, P-OLPD figurant dans le rapport explicatif décrit toutefois une règlementation bien plus stricte, ce qui signifierait donc qu'il y a eu un durcissement[273].

VUD ajoute que « l'adéquation » doit également tenir compte de l'intérêt à l'information et des attentes des personnes concernées. Par exemple, il n'est pas habituel de trouver des déclarations de protection des données sur des cartes de visite, sur du papier à lettres dans des courriels. Dans les situations du quotidien, par exemple au guichet, lorsqu'une personne prend un rendez-vous, il ne devrait pas non plus être obligatoire de renvoyer explicitement à une déclaration de protection des données[274]. C'est dans ce contexte que Bär & Karrer conclut que la règlementation est disproportionnée, qu'elle n'est pas applicable et inutilement compliquée. Selon eux, il suffit de publier les informations sur un site Internet, et cela correspond aux pratiques actuelles[275]. Selon la Raiffeisen, procéder de la sorte permettrait de s'acquitter du devoir d'informer, par exemple dans les conditions générales. Walderwyss mentionne que le devoir d'informer n'exige pas un acte juridique, mais plutôt une déclaration, de manière analogue à ce qui est prévu dans la loi fédérale du 5 octobre 1990 sur l'information des consommatrices et des consommateurs. Par conséquent, la possibilité de consulter les informations suffit.

La Poste critique par ailleurs le fait que le rapport explicatif mentionne la possibilité de satisfaire le devoir d'informer par téléphone. Dans le cas d'une procédure pénale, cela poserait des problèmes bien trop importants en matière de preuves.

Enfin, des participants ont fait remarquer que l'expression « informations les plus importantes » (p. 29 du rapport explicatif) n'était pas claire et qu'il faut la préciser dans le passage du rapport explicatif concerné[276].

Dans leurs commentaires relatifs à l'alinéa 1, voire à l'ensemble de l'ordonnance, l'attention des participants s'est concentrée sur la question de la forme électronique. Dans la perspective de l'avenir et du développement du monde numérique, il faut fixer que les informations peuvent être mises à disposition sous forme électronique et pas uniquement sur papier[277]. ProFonds constate toutefois que le rapport explicatif n'est pas suffisamment clair en ce qui à trait à la façon dont le responsable doit s'acquitter de son devoir d'informer hors du domaine numérique. Lors d'un appel téléphonique, doit-il lire la déclaration de protection des données, longue de plusieurs pages, à haute voix ? D'autres participants souhaitent que l'ordonnance

[271] Organisations : ASSL, auto suisse, FSA, IGEM, suva, Swiss Insights, UPSA, VUD.

[272] Organisations : ASSL, economiesuisse, Swiss Insights, UPSA, usam, VUD.

[273] Organisations : UPSA, GastroSuisse, HotellerieSuisse, ASB, usam (du même avis), ASSL, Swiss Insights.

[274] Et organisations : ASSL, auto suisse, economiesuisse, Swiss Insights, UPSA.

[275] Organisations : AFBS (du même avis), ASA, BNS, Bär & Karrer, economiesuisse, HotellerieSuisse, IGEM, la Poste, Migros, Raiffeisen, SPA, suva, SWICO, swissICT, VUD, Walderwyss.

[276] Organisations : ASB, ASSL, auto suisse, economiesuisse, HotellerieSuisse, Swiss Insights, UPSA.

[277] Organisation: ASB.

explicite que la communication par « voie électronique » est possible, comme le mentionne le rapport explicatif (par exemple sur un site web)[278]. De nos jours, renvoi à un site web ou à des conditions générales semble suffisant[279]. ProFonds fait remarquer qu'il est difficile de comprendre, dans le rapport explicatif, ce que l'on entend par la « bonne pratique » et par le fait que les informations sont « disponibles en un coup d'œil ».

Certains participants sont satisfaits que le P-OLPD évite la rupture de média (« *Medienbruch* »). Il est important de conserver l'art. 13 du projet dans sa forme actuelle puisqu'il faut absolument éviter cette rupture de média[280].

Al. 2

Les milieux économiques se montrent critiques envers l'al. 2 : il est difficile à comprendre, n'apporte aucune valeur ajoutée et est inapplicable[281]. Pour commencer, la VUD relève qu'il est difficile de comprendre en quoi le fait de pouvoir comparer des documents et l'automatisation, mentionnée dans le rapport explicatif, font partie des objectifs de la protection des données[282]. Cette norme ne repose par ailleurs sur aucune base légale selon plusieurs participants[283]. La loi sur la protection des données révisée a fait l'objet d'un examen approfondi par le Parlement et elle est le fruit d'un compromis : il n'est pas admissible de soumettre le devoir d'informer à des exigences supplémentaires par le biais de l'ordonnance[284]. Puisque l'éventuelle utilisation de pictogrammes est volontaire, ils peuvent seulement être utilisés à titre complémentaire. Il n'y a donc pas lieu de poser davantage d'exigences quant à leur utilisation[285].

Bien que les participants reconnaissent globalement qu'il est souhaitable que les pictogrammes utilisés puissent être traités automatiquement, ils rejettent le fait que cela soit fixé dans l'ordonnance. Les pictogrammes servent avant tout à fournir des informations et à améliorer la transparence. Il est donc important que les entreprises puissent les utiliser facilement. L'exigence de la lisibilité par machine ajoute un obstacle supplémentaire[286], ce qui est d'autant moins approprié que la disposition concrétise le devoir d'information, sous peine de sanctions[287]. SWICO ne parvient pas à déterminer de façon certaine si une violation de cet alinéa serait punissable ou non.

Certains participants ne comprennent pas exactement comment « lisible par machine » doit être interprété[288]. Cela pourrait entraîner une certaine insécurité juridique, qui découragerait à

[278] Organisations : ASB, Economiesuisse, VUD.

[279] Organisationa : Curafutura, proFonds, suisa.

[280] Cantons : SO ; partis : PLR.

[281] Organisations : AFBS, ASA, auto suisse, Datenschutzguide.ch.

[282] Organisations: EXPERTsuisse, IGEM, suva, swissICT, VUD, Walderwyss.

[283] Parti: PLR; organisations : Datenschutzguide.ch, EXPERTsuisse, FSA, IGEM, Migros, SPA, SWICO, swissICT.

[284] Organisations : ASB, Economiesuisse, Privacy Icons, VUD.

[285] Organisations : ASB, ASSL, economiesuisse, IGEM, La Poste, suva.

[286] Organisations : ASB (du même avis/ dans le même esprit / par analogie), Migros, SWICO, VUD, Walderwyss.

[287] Organisation : Migros.

[288] Organisations : AFBS, ASA, ASB, ASSL, CFC, economiesuisse, FER, SPA, suva, SWICO, UPSA, VUD.

son tour l'utilisation de pictogrammes[289]. Il n'existe pas de standard pour ce type d'informations[290]. Selon santésuisse aussi, le lien entre pictogrammes et lisibilité par la machine ne semble pas clair.

Selon quelques participants, il y a de plus une erreur dans le raisonnement : les pictogrammes ont pour but d'être plus faciles à interpréter que du texte et de permettre de réagir de façon intuitive à une déclaration de protection des données. S'il faut qu'une déclaration de protection des données soit évaluée automatiquement, ce ne sont pas les pictogrammes qui doivent être lisibles par machine, mais le contenu de la déclaration elle-même, et cette dernière devrait éventuellement être codée en conséquence[291].

La suppression de cet alinéa est demandée. S'il n'est pas entièrement supprimé, le texte devrait au moins préciser que les exigences en matière de lisibilité par machine ne doivent pas être trop élevées. Par exemple, l'ajout d'un texte explicatif en arrière-plan pour les données qui revêtent le format d'une image, ou le formatage d'un pictogramme au format de texte[292], afin qu'ils puissent être traités par un ordinateur, devraient être suffisants[293]. L'ASDPO fait remarquer que des explications supplémentaires devraient être fournies, par exemple dans quel contexte ces pictogrammes seraient utilisés, quels types de pictogrammes pourraient être utilisés et s'il faudrait qu'ils soient reconnus par le PFPDT.

La Poste apprécierait que l'on précise, en s'appuyant sur l'art. 13 RGPD, que le devoir d'informer n'exige pas de nommer précisément les pays destinataires en cas de communication des données à l'étranger. Si la sécurité des données n'est pas suffisamment assurée dans les États destinataires visés, il faut que les informations fournies permettent aux personnes concernées de déterminer le pays auquel les données ont été communiquées et les garanties que ce pays offre en matière de protection des données.

3.2.14 Art. 14 P-OLPD : Disposition particulière relative au devoir d'informer des organes fédéraux lors de la collecte des données personnelles

Des participants font remarquer qu'en plus du cas des questionnaires, il existe d'autres contextes dans lesquels les personnes ne sont pas tenues de fournir des renseignements. Cela devrait ressortir plus clairement de l'ordonnance[294]. Certains participants notent que l'obligation de mentionner le caractère facultatif devrait seulement exister quand les circonstances ne permettent pas de le déduire[295]. swissICT critique la confusion entre la protection des données et les obligations légales de collaborer : la protection des données a son importance, indépendamment du fait que des informations sont communiquées volontairement ou non.

[289] Organisations : ASB, Curafutura, DFS, economiesuisse, Migros, Privacy Icons, VUD.

[290] Organisations : IGEM, suva, SWICO, swissICT, VUD.

[291] Organisations : IGEM, suva, VUD.

[292] Webfont.

[293] Organisations : ASB, Economiesuisse, Privacy Icons, VUD.

[294] Organisations : ASDPO, HDC, swissprivacy.law.

[295] Organisations : ASA, CFF, Curafutura, IGEM, SNP, suva, SWICO, VUD, Walderwyss.

3.2.15 Art. 15 P-OLPD : Informations lors de la communication des données personnelles

FRC approuve explicitement cet article, même s'il fait l'objet de critiques de la part d'autres participants. D'après ces derniers, il est dépourvu de base légale ou il devrait figurer au niveau de la loi[296]. Plus précisément, le Parlement a réglé la question de la communication de données personnelles de façon suffisamment claire dans plusieurs articles de la loi, sous forme de principes et dans le respect de l'approche fondée sur les risques. Il a tenu à dégager une marge de manœuvre suffisante pour que chaque responsable puisse l'appliquer à sa façon[297].

La Poste fait remarquer que l'art. 15 P-OLPD contredit l'art. 19, al. 1, nLPD. Pharmasuisse note que la nLPD instaure uniquement une obligation d'informer le destinataire à la demande de la personne concernée. D'autres participants avancent que les principes de l'art. 6 nLPD devraient s'appliquer : il prévoit que celui qui traite des données personnelles doit s'assurer de leur exactitude[298].

Pour certains, l'article est superflu parce que le responsable doit s'assurer du respect des principes de protection des données. L'information serait de toute façon inutile lorsqu'il s'agit de traitements de données prévus par la loi[299]. Le destinataire doit s'assurer que les données sont exactes et respecter les principes de traitement des données. Une information appropriée de la part de la personne qui transmet l'information irait à l'encontre de cette obligation, ou aurait pour conséquence qu'une mesure de vérification de l'exactitude devienne le seul critère valable, ce qui est contraire au texte de la loi[300].

Le RGPD ne prévoit en outre pas un tel devoir d'informer pour les responsables privés : il s'agit d'un Swiss Finish[301]. Dans le domaine privé, il n'y a pas lieu de s'appuyer sur la directive UE 2016/680, qui mentionne explicitement en son art. 7, al. 2, les « autorités compétentes »[302]. Il faudrait au moins limiter la réglementation proposée aux organes fédéraux[303]. À ce sujet, les CFF font remarquer que la directive UE 2016/680 doit uniquement s'appliquer dans le domaine pénal et qu'elle ne saurait être utilisée comme base légale dans d'autres domaines.

La disposition est considérée comme trop éloignée de la pratique[304], de par son caractère démesuré et trop formaliste[305]. Les exigences supplémentaires auxquelles serait soumis tout type de communication en lien avec des données personnelles sont trop élevées[306] et doivent même s'appliquer en l'absence de risque perceptible[307]. Cette disposition va à l'encontre

[296] Cantons : LU; partis : Le Centre, PLR; organisations : ASA, ASB, ASSL, auto suisse, CP, curafutura, Datenschutzguide.ch, DFS, economiesuisse, EPS, EXPERTsuisse, FSEP, HDC, IGEM, la Poste, Migros, pharmasuisse, proFonds, Rega, Ringier, santésuisse, Scienceindustries, SDV, SPA, SSMD, suisa, suva, SWICO, Swiss Insights, swissICT, swissstaffing, UPSA, usam, UTP, UVS, veb.ch, vsi, VUD.

[297] Organisations : ASB, economiesuisse, Scienceindustries suisse.

[298] Cantons : BE; organisations : Bär & Karrer, proFonds, suva, swissICT.

[299] Organisations : ASA, ASSL, curafutura, Rega, UPSA, UTP, VUD.

[300] Organisations : H+, IGEM.

[301] Organisations : ASB, ASSL, Digitialswitzerland, Economiesuisse, EXPERTsuisse, FSA, HotellerieSuisse, IGEM, Ringier, Scienceindustries suisse, suva, SWICO, SwissHoldings, UPSA, VUD.

[302] Cantons : TG (de façon implicite) ; organisations : ASSL, economiesuisse, HotellerieSuisse, UPSA.

[303] Organisations : ASB, Economiesuisse, EXPERTsuisse.

[304] Organisations : ASA, DFS, H+, HÄRTIG Rechtsanwälte, IGEM, Migros, SDV, suva, SwissHoldings, swissICT.

[305] Organisations : CP, SDV.

[306] Organisations : ASB, CP, curafutura, economiesuisse, IGEM, la Poste, Rega, suva, SwissHoldings, swissICT, VUD.

[307] Organisation : CP.

des efforts entrepris par le Conseil fédéral en vue de promouvoir la numérisation et la capacité d'innovation de la Suisse dans l'intérêt de sa place économique[308].

Les participants regrettent en particulier qu'il faille informer le destinataire de l'exhaustivité des données. Dans les faits, cela signifie que les responsables ne pourront pas communiquer de données incomplètes[309]. Certains font remarquer qu'il faudra veiller, lors de l'application de la disposition, à ce que les exigences quant au niveau de détail des informations à communiquer ne soient pas trop élevées[310]. D'autres participants estiment encore que la norme doit se limiter aux données dont le traitement présente un risque résiduel[311].

Dans tous les cas, il faudrait au moins retirer le sous-traitant de cet article étant donné qu'il n'est pas soumis au devoir d'informer d'après la nLPD[312] et qu'il n'est souvent pas en possession des informations nécessaires[313]. D'après SWICO, il appartient au responsable de garantir le respect des principes de protection des données.

Enfin, Forum PME considère que cette règlementation n'est pas suffisamment claire et qu'elle mérite interprétation. Pour la SPA, il est difficile de savoir ce que l'on entend par la « fiabilité » des données personnelles.

3.2.16 Art. 16 P-OLPD : Informations sur la rectification, l'effacement ou la destruction, ainsi que sur la limitation du traitement des données personnelles

Deux participants à la procédure de consultation estiment que l'article ne va pas suffisamment loin. Il est à leur sens capital que la personne concernée soit informée sans délai de la rectification, de l'effacement ou de la destruction de ses données[314]. D'autres relèvent que les obligations prévues à l'art. 16 P-OLPD figuraient dans le projet de nLPD et ont été expressément rejetées par le Parlement[315]. Il n'existe pas non plus de base légale à leurs yeux[316]. En outre, le droit des personnes concernées de « limiter » le traitement de leurs données personnelles évoqué l'art. 18 RGPD et n'existe pas non plus dans la nLPD[317]. À cela s'ajoute le fait que la rectification, l'effacement, la destruction et la limitation du traitement des données personnelles sont effectués dans l'intérêt de la personne concernée[318]. Le responsable doit de toute façon respecter les principes du traitement des données ou s'assurer de leur respect[319].

En parallèle au refus de principe de la norme en raison de l'absence de base légale ou de son caractère redondant, certains participants ont émis des critiques plus détaillées. HDC indique que ces obligations devraient être limitées dans le temps. Il faut préciser que le respon-

[308] Organisations : HDC, SwissHoldings.

[309] Organisations : H+, IGEM, la Poste, suva, veb.ch.

[310] Organisations : ASPS, CURAVIVA, INSOS, IS, senesuisse, Spitex.

[311] Organisations : HDC, SwissHoldings.

[312] Cantons : BE; organisations : Curafutura, FMH, pro Fonds, santésuisse, SDV, SWICO, swissstaffing, UVS, VUD.

[313] Organisations : IGEM, suva, swissICT, UVS, VUD.

[314] Organisations : DigiGes, FRC.

[315] Canton : BE; partis : Le Centre, PLR; organisations : ASB, ASSL, economiesuisse, HotellerieSuisse, proFonds, Rega, suisa, Swiss Insights, UPSA, usam, UVS, veb.ch, VUD.

[316] Canton : BE; partis : Le Centre, PLR; organisations : ASSL, Creditreform, curafutura, HotellerieSuisse, proFonds, SSMD, suisa, Swiss Insights, UPSA, UTP.

[317] Organisations : HotellerieSuisse, Rega, VUD.

[318] Organisations : Creditreform, UTP.

[319] Organisations : ASSL, Creditreform, Swiss Insights, UPSA, UTP.

sable du traitement n'a pas l'obligation de conserver une copie des données communiquées et des destinataires. UPSV note que la notion d'« efforts disproportionnés » doit être décrite plus précisément dans le rapport explicatif ou dans le texte de l'ordonnance lui-même. La marge d'interprétation est trop grande et laisse entrevoir la possibilité de renoncer à l'information pour éviter une charge de travail supplémentaire. DigiGes fait remarquer que l'article ne délie pas le responsable de son devoir d'informer la personne concernée et qu'il faudrait par conséquent le préciser.

3.2.17 Art. 17 P-OLPD : Réexamen d'une décision individuelle automatisée

Plusieurs participants à la procédure de consultation saluent cette disposition. Certains ont souligné que les décisions automatisées peuvent entraîner des injustices[320]. Cet art. 17 devrait permettre, à juste titre, d'éviter que les personnes concernées renoncent à demander un réexamen. D'autres participants se sont montrés critiques. Selon eux, le Parlement a déjà réglé de façon claire le devoir d'informer en cas de décision individuelle automatisée à l'art. 21 nLPD, sous forme de principes et dans le respect de l'approche fondée sur les risques. Par ailleurs, il a volontairement tenu à laisser une marge d'appréciation aux responsables du traitement pour la mise en œuvre de la disposition. D'autres prescriptions qui figurent dans le projet ne reposent pour certains sur aucune base légale[321]. Certains estiment que cet article constitue une atteinte à l'autonomie privée et qu'il devrait être inscrit au niveau de la loi[322].

Pour des participants, la règlementation est en outre basée sur de fausses dispositions légales : il n'existe pas d'interdiction générale de la discrimination. Dans la mesure où une telle interdiction est directement dérivée des droits fondamentaux de la Constitution, elle n'est pas admissible dans ce contexte parce que les droits constitutionnels n'ont pas d'effet horizontal direct. Une discrimination devient critiquable sur le plan juridique si est purement subjective et qu'il n'existe pas de critères de délimitations objectifs convaincants[323]. D'après le canton de Lucerne, il faut questionner la conformité de cet article à la loi, car l'art. 61 nLPD prévoit une disposition pénale.

Asut ajoute qu'il est difficile d'interpréter ce que signifie le fait que la personne « ne peut pas être désavantagée pour ce motif ». DFS aimerait que l'on dresse, à titre d'exemple, une liste des désavantages possibles. L'Association de commerce estime que la mise en œuvre de cette partie de la phrase n'est pas réalisable. Dans la plupart des cas, la personne concernée se sent désavantagée par la décision individuelle automatisée. De plus, un fournisseur a le droit de choisir ses partenaires contractuels. La norme est toutefois expressément approuvée. Il est néanmoins important de limiter au maximum les discriminations dues aux décisions individuelles automatisées. En ce sens, certains participants se félicitent que le Conseil fédéral démontre, dans l'ordonnance d'exécution, qu'il tient à ce que les personnes qui demandent le réexamen d'une décision individuelle automatisée par une personne physique ne puissent pas être désavantagées[324].

HDC est d'avis que l'interdiction de désavantager les personnes, fixée à l'art. 17 P-OLPD, devrait être concrétisée. L'autorité cantonale de protection des données de Fribourg fait également remarquer que l'on ne sait pas si une demande de réexamen au sens de l'art. 17 P-OLPD peut conduire à une nouvelle décision. Le canton de St-Gall estime qu'il faudrait

[320] Parti : PS; organisations : FRC, USS.

[321] Cantons : LU ; organisations : asut, Economiesuisse.

[322] Organisations : ASB, Bär & Karrer (du même avis), Economiesuisse.

[323] Organisations : ASB, Bär & Karrer (du même avis), Economiesuisse.

[324] Parti : PS, organisations : FRC, USS.

détailler la disposition en précisant que les décisions individuelles automatisées ne peuvent pas déployer leurs effets avant qu'un certificat de contrôle attestant la potentielle nouvelle décision n'ait été établi.

De façon générale, les participants notent que cette réglementation pourrait encourager les plaintes abusives contre les responsables[325]. Cette question ne devrait pas être réglée dans le P-OLPD parce qu'elle porte sur un sujet de nature générale, qui joue un rôle équivalent dans tous les domaines du droit. Seule la pratique établie des tribunaux fédéraux permet de garantir une sécurité du droit suffisante[326].

USS voit un réel risque dans le fait que, dans le domaine de l'emploi, de plus en plus de décisions sont automatisées, et il demande une meilleure protection contre les licenciements (augmentation des indemnités à 24 mois de salaire et inscription d'un droit au réengagement à l'art. 336a CO).

3.2.18 Art. 18 P-OLPD : Forme et conservation de l'analyse d'impact relative à la protection des données personnelles

PS approuve le délai de conservation proposé par le Conseil fédéral et demande qu'il ne soit pas raccourci. DFS souhaite quant à lui une extension du délai à cinq ans, au motif que l'analyse d'impact relative à la protection des données est un instrument particulièrement utile pour la réduction systématique des risques et qu'elle constitue l'une des nouveautés les plus importantes de la nLPD. Si un traitement des données abusif entraîne des dommages pour la personne concernée et que des questions de responsabilité se posent, l'analyse d'impact pourrait être un document qui servirait à vérifier les responsabilités. L'ASDPO est surpris que les durées de conservation ne soient pas harmonisées dans l'ensemble du P-OLPD et propose également un délai de 5 ans dans le cas présent. Le délai de conservation fixé paraît difficile à comprendre pour Bär & Karrer, qui suggère d'adopter des délais uniformes afin de simplifier la procédure au sein des entreprises.

D'autres participants se montrent plus critiques. Ils regrettent notamment que l'obligation de conserver l'analyse d'impact relative à la protection des données personnelles ne repose pas sur une base légale : le législateur a volontairement renoncé à inscrire ce type d'obligation de documentation générale dans la loi au profit d'une obligation de tenir un registre des activités de traitement[327]. Le canton de Schwyz relève qu'en leur qualité de document officiel, les analyses d'impact destinées aux organes fédéraux doivent être soumises aux règles générales de conservation des documents et ne devraient pas être réglées à part dans l'OLPD. Certains participants regrettent qu'il s'agisse là encore d'un Swiss Finish puisque le RGPD ne prévoit aucune obligation de cet ordre[328].

Cette règle est par ailleurs contraire au principe « nemo tenetur »[329] parce que l'analyse d'impact relative à la protection des données personnelles qui est conservée pourrait être utilisée

[325] Organisations : ASB, Economiesuisse, swissICT.

[326] Organisations : ASB, Economiesuisse.

[327] Organisations : AFBS, ASB, ASSL, BNS, Bär & Karrer, CP, Creditreform, economiesuisse, EPS, FSA, FSEP, HÄRTING, HotellerieSuisse, IGEM, Migros, pharmasuisse, SPA, suisa, suva, swissICT, swissstaffing, UPSA, usam, UVS, vsi, VUD, Walderwyss.

[328] Organisations : ASSL, Migros, UPSA.

[329] Le principe « nemo tenetur » est considéré comme l'un des principes fondamentaux d'une procédure pénale équitable. D'après celui-ci, personne ne doit être tenu de contribuer à sa propre incrimination.

en tant que preuve contre le responsable dans le contexte de la de pièces ou dans le cadre de l'administration des preuves[330].

Un raccourcissement du délai est demandé *a minima*. Les participants estiment qu'il est trop long[331], en particulier parce que le traitement des données tel qu'il est défini à l'art. 5, let. d, nLPD comprend l'archivage[332]. Certains sont d'avis que rien ne justifie un délai de conservation aussi long au vu des principes de la proportionnalité du traitement des données et de la minimisation des données[333]. Le canton de Zurich fait, d'une part, remarquer que les résultats de l'analyse d'impact seraient directement intégrés dans le traitement des données évalué et, d'autre part, que le tableau dressé dans l'analyse d'impact deviendrait très rapidement obsolète. Quelques participants ajoutent que l'on pourrait limiter la conservation jusqu'au moment où le traitement des données prend fin, puisqu'après cela, les droits de la personne concernée ne peuvent plus être violés[334]. Asut suggère qu'il faudrait laisser le responsable déterminer un délai de conservation adapté au cas particulier et ce en tenant compte du fait qu'il risque de devoir s'acquitter de la charge de la preuve. Une autre proposition consiste à adapter la durée de conservation au besoin de protection des données[335]. Enfin, si ce délai est conservé, certains veulent ajouter que l'analyse d'impact devra être conservée pendant deux ans « au moins », afin d'éviter qu'une conservation plus longue ne soit contraire aux prescriptions de protection des données[336].

En outre, un certain nombre de participants souhaitent que l'ordonnance[337] explicite le fait que la forme écrite peut aussi comprendre des documents sous forme électronique qui servent de preuve par le texte. Il ne suffit pas de le mentionner dans le rapport explicatif[338]. Quelques-uns déplorent le fait qu'il faille interpréter la forme écrite au sens du CO (arrêt du TAF A-3548/2018 du 19 mars 2019, consid. 4.8.4) et qu'une signature soit nécessaire. Il devrait être possible de produire et de conserver l'analyse d'impact sous forme électronique, à condition qu'elle soit conservée en sécurité et disponible en tout temps[339]. Exiger la forme écrite n'est pas nécessaire et n'est plus d'actualité[340]. D'autres estiment qu'on ne peut déterminer si un simple courriel suffit à remplir le critère de la forme écrite ou s'il faut une signature électronique. Il vaudrait la peine de le préciser. Les exigences quant à la forme écrite ne devraient toutefois pas être trop élevées[341]. Si le critère de la forme écrite est conservé, il faudrait préciser qu'elle doit être interprétée de manière plus large que selon la règle formelle des art. 12 ss CO[342].

Une critique va plus en détail et dénonce le fait que la réglementation part du principe que l'analyse d'impact relative à la protection des données personnelles ne serait jamais mise à

330 Organisations : ASB, Economiesuisse.

331 Cantons : ZH; organisations : ASP, ASPS, Creditreform, Curaviva Schweiz, EPS, FSEP, INSOS, IS, senesuisse, Spitex suisse.

332 Organisation : swissprivacy.law.

333 Organisations : ASB, Economiesuisse.

334 Organisations : ASP, Creditreform, EPS, FSEP.

335 Organisations : Classtime, vsi.

336 Organisations : BNS, Economiesuisse, Walderwyss.

337 Et pas uniquement le rapport explicatif.

338 Cantons : BE; organisations : AFBS, ASA, ASB, ASDPO, ASSL, BNS, Bär & Karrer, curafutura, DFS, economiesuisse, FER, HÄRTING, HotellerieSuisse, la Poste, proFonds, Ringier, SPA, suva, swissICT, swissprivacy.law, UPSA, vsi, VUD, Walderwyss.

339 Organisations : ASDPO, curafutura, HDC, proFonds, swissprivacy.law, Walderwyss.

340 Organisations : ASA, Asut, curafutura, swissprivacy.law.

341 Organisations : Association de commerce, Asut, Bär & Karrer, santésuisse.

342 Organisations : HDC, swissprivacy.law.

jour, ce qui ne correspond pas à la pratique. Il n'est d'ailleurs pas précisé comment procéder s'il existe plusieurs versions : il faudrait ajouter qu'il faut se référer à la version la plus récente[343]. Curafutura demande que les organes fédéraux ne doivent pas établir une analyse d'impact relative à la protection des données personnelles si les données sont traitées dans le cadre prévu par la loi. La FMH estime que cette disposition devrait préciser le libellé de l'art. 22, al. 2, let. a, nLPD pour définir sans équivoque en quoi consiste un traitement de données « à grande échelle ».

3.2.19 Art. 19 P-OLPD : Annonce des violations de la sécurité des données

Al. 1

L'art. 24, al. 1, nLPD ne prévoit une annonce des violations de la sécurité des données que lorsqu'il existe un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Il s'écarte donc volontairement de l'art. 33 RGPD. Cependant, l'art. 19 P-OLPD reprend la majorité des dispositions de l'art. 33 RGPD. Celles-ci servent principalement aux responsables également soumis au RGPD, mais pour les autres, elles constituent des dispositions supplémentaires inutiles qui engendrent un surcroît de travail[344]. L'indication du moment et de la durée de la violation des données vont tout particulièrement plus loin que le RGPD : il s'agit d'un Swiss Finish[345]. DigiGes souligne en revanche que ces indications ne dépassent pas le cadre de la loi. En effet, les indications ne doivent être fournies que dans la mesure où le moment et la durée peuvent être déterminés et si elles sont d'une importance capitale pour apprécier la gravité de la violation. La suva considère que la let. a va plus loin que le RGPD, mais que cela ne devrait pas poser de problème en pratique[346].

D'autres obligations vont au-delà de l'art. 24, al. 4, nLPD. Les critères inscrits aux let. b à d ne découlent pas de la loi selon certains, il n'y a donc pas de base légale[347]. L'atténuation d'un grand nombre de ces dispositions supplémentaires (via l'ajout de « dans la mesure du possible ») est peu judicieuse. L'objectif de cet article est que l'autorité de surveillance soit informée rapidement, tout comme les personnes concernées, et que des mesures de protection des données personnelles soient prises immédiatement. L'art. 24 nLPD n'a pas besoin de la concrétisation contenue dans cet article de l'ordonnance[348]. Certains sont d'un avis divergent et trouvent cet ajout utile du fait qu'il n'est souvent pas possible de réunir ces informations[349]. DigiGes affirme que les informations mentionnées aux lettres a à g sont nécessaires pour que le PFPDT puisse dresser un tableau complet du cas de violation de la sécurité des données. Cet aspect est aussi souligné dans le rapport explicatif. L'ASDPO estime que les informations figurant aux let. b à d doivent être fournies dans tous les cas et qu'il faut par conséquent supprimer « dans la mesure du possible ».

Asut note que la formulation des let. e et f n'est pas claire et qu'elles ne traduisent pas le fait qu'il faille seulement annoncer au PFPDT les cas qui entraînent « vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée »[350]. D'après certains, la let. e devrait être refomulée de la sorte en allemand : « *die Folgen für*

[343] Organisations : BNS, IGEM, suva, VUD, Walderwyss.

[344] Cantons : UR, AR, AG, BL, GR, NW, SH, SZ, VD, ZH; organisations : Préposé à la protection des données de SZ, OW et NW, privatim.

[345] Organisations : ASB, ASSL, auto suisse, Digitalswitzerland, Ringier, suva, Swiss Insights, UPSA.

[346] Organisations : ASB, suva.

[347] Cantons : BS; organisations : ASP, Association de commerce, Creditreform, FSEP, Ringier, SPA, usam, vsi.

[348] Cantons : AG, AR, BL, BS, GR, NW, OW, SH, VD, ZH; organisation: privatim.

[349] Organisations : ASB, Economiesuisse, SPA.

[350] Et organisation: HÄRTING.

die betroffenen Personen, von welchen ein hohes Risiko ausgeht » (les conséquences pour les personnes concernées qui entraînent un risque élevé). Cette formulation couvre également les risques éventuels[351]. De plus, l'art. 33, al. 3, let. c, RGPD parle de « conséquences probables ». Il faudrait aussi reprendre cette expression dans le P-OLPD : concrètement, le responsable est seulement dans la mesure d'émettre des hypothèses quant aux conséquences[352]. D'autres souhaitent en revanche que la let. e soit aussi complétée par « dans la mesure du possible » parce qu'il n'est pas toujours envisageable de déterminer immédiatement et définitivement les conséquences et les éventuels risques que présente une violation de la sécurité des données au moment où on la constate[353]. De plus, il faudrait parler à la let. f de « risques » et non pas de « conséquences » [354]. swissICT relève que même si l'on remédie au manquement, il faudrait malgré tout et dans le même temps atténuer les conséquences ou les dommages causés[355]. Economiesuisse souligne qu'en ajoutant « le cas échéant » à cet alinéa, on pourrait indiquer qu'il suffit d'annoncer les mesures effectivement mises en place.

Swissprivacy.law tient à ce que l'on précise qu'il faut uniquement fournir toutes les informations si l'annonce des violations de la sécurité des données est obligatoire. Lorsque le responsable informe le PFPDT de manière volontaire, il ne doit pas forcément donner toutes les informations dont l'al. 1 dresse la liste. D'aucuns demandent une réglementation « *de minimis* », qui exclut les cas dans lesquels le PFPDT n'a pas de marge de manœuvre : elle permettrait d'économiser des ressources[356].

Al. 2

La précision « lors de la détection de la violation de la sécurité des données » n'a que peu d'intérêt. En effet, à ce moment-là, on sait d'expérience que le responsable ne dispose pas encore de toutes les informations nécessaires car elles ne peuvent être réunies qu'avec le temps[357]. À l'inverse, l'ASDPO souhaite qu'il soit clairement indiqué que le responsable du traitement doit annoncer les violations dans les meilleurs délais, pas seulement au moment de la détection de la violation.

Al. 3

Un certain nombre de participants à la procédure de consultation font remarquer que la loi prévoit que la personne concernée soit seulement informée lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige. En revanche, l'ordonnance prévoit dans tous les cas la communication des informations visées à l'al. 1, let. a, e, f et g. Cet alinéa ne repose par conséquent pas sur une base légale[358]. C'est pourquoi FER propose de clairement indiquer que cet alinéa vaut uniquement si la personne concernée doit être informée conformément à la loi[359]. PC souhaite quant à lui que le moment et la durée de la violation soient aussi communiqués à la personne concernée afin que cette dernière puisse estimer au mieux la

[351] Organisations : Economiesuisse, IGEM, SPA, suva, swissICT.

[352] Organisations : Association de commerce, FER.

[353] Organisations : ASP, Association de commerce, Creditreform, FSEP, usam, vsi.

[354] Organisations : ASB, Economiesuisse, SPA.

[355] Et organisation : HÄRTING.

[356] Organisations : ASB, Economiesuisse, IGEM, SPA, suva, VUD.

[357] Organisations : IGEM, santésuisse, suva, VUD.

[358] Organisations : ASP, ASSL, Association de commerce, asut, auto Swiss, economiesuisse, FER, FSEP, SPA, Swiss Insights, UPSA, vsi.

[359] Organisation : FER.

gravité de la violation et les risques qu'elle engendre. L'ASDPO tient à ce que les informations figurant aux let. b et c soit également communiquées à la personne concernée, car elles peuvent les aider à déterminer l'étendue de l'incident et prendre les mesures qui s'imposent[360]. D'autres acteurs demandent de supprimer la mention de la let. g parce ce type d'information pourrait faciliter les cyberattaques et parce qu'il y a plusieurs personnes de contact dans les grandes entreprises[361].

Al. 4

HDC rappelle que l'art. 24, al. 6, nLPD prévoit que l'annonce peut uniquement être utilisée contre la personne tenue d'annoncer dans le cadre d'une procédure pénale si celle-ci y a consenti. Il faudrait clarifier que lorsqu'il s'agit d'une personne morale, la personne morale en tant que telle et toutes les personnes physiques qui en font partie sont tenues de faire une annonce. Le canton de Fribourg souhaite éviter que toute annonce se retrouve sur la place publique de manière prématurée. Le Tribunal fédéral a toutefois jugé qu'une annonce des violations de la sécurité des données était soumise au principe de la transparence (ATF 1C_500/2020 du 11 mars 2021). Puisque cette annonce deviendrait obligatoire, il serait opportun d'introduire une limitation temporelle concernant l'accès à ce type d'annonces.

Al. 5

Selon DigiGes, il est important que les violations soient documentées pour toutes les parties impliquées, comme prévu à l'art. 19, al. 5, P-OLPD. L'ASDPO juge qu'il serait utile d'exiger une documentation de toutes les violations, de manière à ce que le PFPDT ou d'autres autorités, en cas de contrôle, soient en mesure de vérifier si une violation aurait dû être annoncée alors qu'elle ne l'a pas été. Certains participants trouvent la disposition imprécise puisqu'elle ne permet pas de déterminer si toutes les violations doivent être documentées ou uniquement celles qui doivent être annoncées au PFPDT[362]. D'autres partent du principe que seules les violations devant être annoncées devraient être documentées. Le sens de la norme n'apparaît donc pas très clairement. En effet, si le PFPDT s'intéresse à une violation qui doit être annoncée, il se renseignera de toute façon[363].

De nombreuses voix s'élèvent pour demander une suppression de l'obligation de documenter figurant à l'al. 5, faute de base légale[364]. L'obligation d'annoncer les violations de la sécurité des données est réglementée de façon suffisamment claire au niveau de la loi, sous forme de principes et dans le respect de l'approche fondée sur les risques. Par conséquent, le Parlement a cherché à volontairement octroyer une marge de manœuvre adéquate aux responsables du traitement pour l'exécution au cas par cas[365]. L'art. 24 nLPD ne prévoit pas d'obligation de documenter et de conserver les informations liées à une violation de la sécurité des données[366], et ce n'est pas non plus le cas du RGPD. Cet alinéa est donc un Swiss Finish[367].

[360] Et organisation: Swimag (du même avis).

[361] Organisations : AFBS, swissICT.

[362] Organisations : ASDPO, swissprivacy.law.

[363] Organisations : BNS, H+, HDC, Rega, suva, SWICO.

[364] Organisations : AFBS, ASB, ASP, ASSL, Association de commerce, asut, auto suisse, BNS, Bär & Karrer, Creditreform, economiesuisse, EXPERTsuisse, FSA, FSEP, H+, IGEM, Migros, pharmasuisse, Rega, Scienceindustries, SPA, suisa, suva, SWICO, SwissHoldings, swissICT, swissprivacy.law, swissstaffing, UPSA, usam, UVS, veb.ch, vsi, VUD, Walderwyss.

[365] Organisation: ASB.

[366] Organisations : HDC, Rega.

[367] Organisations : ASSL, auto suisse, Digitalswitzerland, Migros, Scienceindustries, Swiss Insights, SwissHoldings, UPSA.

Par ailleurs, l'obligation est bien trop étendue puisque « tous les faits relatifs aux incidents » devront être documentés[368]. Cette précision induit en erreur en suggérant qu'il faudrait rechercher des faits qui ne figurent pas dans la liste de l'al. 1, let. a à g, tout spécialement du fait de l'obligation de documenter[369]. AFBS note que si cet alinéa était conservé, il faudrait préciser que le responsable doit uniquement fournir des informations dont il a connaissance. On ne peut pas attendre qu'il effectue des recherches auprès d'externes.

Plusieurs participants à la procédure de consultation réclament un raccourcissement de la durée de conservation de la documentation[370]. Certains ajoutent qu'elle devrait être conservée conformément aux règles en vigueur qui s'appliquent aux autorités de surveillance[371]. D'autres souhaitent que les délais de conservation soient harmonisés dans l'ensemble de l'ordonnance, y compris celui figurant à cet alinéa[372]. D'autres encore estiment qu'il faut rallonger ce délai à cinq ans du fait que l'annonce pourrait être pertinente en cas d'action en responsabilité[373]. DigiGes souligne l'importance de ce délai pour la personne concernée car il lui permet de se défendre en recourant aux voies de droit. Economiesuisse demande de préciser qu'il faut uniquement conserver une trace des violations devant être annoncées.

D'aucuns regrettent la mauvaise interprétation de l'adverbe « vraisemblablement » (art. 24, al. 1, nLPD) dans le rapport explicatif, où il est écrit que la violation doit être annoncée « même en cas de doute, pour les cas dans lesquels on ne peut exclure l'existence d'un risque élevé ». Cela présuppose qu'une violation de la sécurité des données entraînerait selon toute probabilité un risque élevé[374]. Il s'agit d'un pléonasme étant donné que la notion de « risque » en elle-même comporte un élément de probabilité puisqu'elle sert à exprimer à quel point il est possible que la violation provoque des dommages. La probabilité doit donc être d'un certain niveau[375]. Ainsi « vraisemblablement » ne signifie en aucun cas que l'annonce doit se faire « même en cas de doute », lorsqu'on ne peut pas exclure l'existence d'un risque élevé. Bien au contraire, la violation ne doit être annoncée que lorsque le risque qu'il y ait effectivement eu une violation des droits de la personne concernée est bien plus élevé que l'éventualité qu'il n'y ait pas de violation des droits[376]. C'est-à-dire, concrètement, dans les cas où il est très probable que la violation de la sécurité des données entraîne un risque élevé[377]. Le Conseil fédéral dépasse d'après eux ici les limites posées par le législateur[378]. La FMH aimerait que la clarification apportée ci-dessus à l'adverbe « vraisemblablement » soit intégrée à l'ordonnance.

[368] Organisations : Bär & Karrer, proFonds.

[369] P. ex. organisations : Bär & Karrer, suva. Von Walderwyss considère que cette notion est floue.

[370] Organisations : ASA, ASP, Creditreform, curafutura, FSEP, proFonds, Ringier, santésuisse, vsi, Walderwyss.

[371] Cantons : ZH ; organisation : Sgv.

[372] Organisations : ASA, Bär & Karrer, curafutura, FMH, Ringier, Walderwyss.

[373] Organisations : ASDPO, DFS, Swimag.

[374] Et non pas que « même en cas de doute, pour les cas dans lesquels on ne peut exclure l'existence d'un risque élevé ». Organisations : ASB, auto suisse, economiesuisse, vsi.

[375] Organisations : ASB, IGEM, suva, VUD.

[376] Organisationen: AGVS, Creditreform, SLV, Swiss Insights, vsi.

[377] Organisations : Economiesuisse, SPA.

[378] Organisations : UPSA, Creditreform, ASSL, Swiss Insights, vsi.

3.2.20 Art. 20 P-OLPD : Modalités

Plusieurs participants considèrent comme positif le renforcement des droits d'accès des particuliers opéré dans le P-OLPD puisqu'il s'agit d'un principe essentiel de la protection des données[379]. La Stiftung für Konsumentenschutz souligne que sans droits d'accès, les personnes concernées ne peuvent pas savoir lesquelles de leurs données personnelles sont traitées. En ce sens, il convient de restreindre au minimum le droit d'accès[380] et de veiller à ne pas inutilement compliquer son exercice[381]. Il est par ailleurs important que cet instrument ne puisse pas être utilisé de manière abusive[382].

D'autres participants sont d'avis que cet article n'apporte aucune valeur ajoutée puisque les art. 25 et 26 nLPD règlent déjà de façon détaillée le droit d'accès et ses limites. Les éléments concrets réglés à l'art. 20 P-OLPD vont plus loin que nécessaire[383]. Certains relèvent aussi que la portée et le but du droit d'accès découlent des dispositions de l'art. 25, al. 2, nLPD[384].

Un autre point relevé est qu'il faudrait ajouter la possibilité de fournir les renseignements sous une forme permettant d'en établir la preuve par un texte[385]. Cette formulation entend en particulier couvrir la forme électronique, qui est par ailleurs explicitement mentionnée dans le rapport explicatif. D'après HDC, l'exigence de la forme écrite ne se justifie pas dans tous les cas, la forme électronique pouvant généralement suffire. Rien ne justifie que le responsable du traitement ait besoin d'une signature manuscrite en lien avec la demande d'accès.

Bien que la possibilité de la forme électronique soit mentionnée dans le rapport explicatif, il vaudrait la peine de le préciser dans l'ordonnance afin d'éviter de faire naître des doutes quant à l'application du droit[386]. Par ailleurs, la SPA estime que le rapport explicatif devrait préciser si la « forme numérique » doit être comprise comme une « forme électronique », dans le sens d'une forme écrite. Swimag exprime le même souhait, en ajoutant qu'il faudrait que cela soit précisé dans l'ordonnance. Creditreform fait toutefois remarquer que la révision de l'OLPD ne constitue pas le cadre adapté pour une telle décision de principe[387].

Al. 1

Certains ont émis le souhait que la demande de renseignement puisse se faire tant par oral que par écrit. L'art. 25 nLPD dispose uniquement que la personne puisse « demander » si des données personnelles la concernant sont traitées, formulation qui couvre à la fois l'oral et l'écrit. Cela permettrait aux personnes pour qui la forme écrite constitue un obstacle difficile ou insurmontable de bénéficier elles aussi d'un moyen de faire valoir leur droit. Permettre au responsable du traitement de déterminer la forme de la demande pourrait conduire à des décisions arbitraires[388]. SWICO fait remarquer qu'en pratique, il n'est pas forcément utile de le préciser puisque la demande de renseignement devrait toujours pouvoir se faire par oral et

[379] Parti : PVS; organisations : DigiGes, Stiftung für Konsumentenschutz.

[380] Parti : PVS.

[381] Organisations : DFS, FRC.

[382] Organisation: DFS.

[383] Cantons : AR, AG, ZH, UR, SH, VD; organisation : privatim.

[384] Cantons : AG, AI, AR, BS, GL, GR, NW, OW, SH, SZ, UR, VD, ZH; organisation : VUD.

[385] Cantons : SG; organisations : ASSL, auto suisse, Creditreform, HÄRTING, SPA, SWICO, Swiss Insights, swissstaffing, UPSA, vsi, VUD.

[386] Cantons : SG, organisations : Economiesuisse, FER, HÄRTING, SPA, SWICO, Swimag, Swiss Insights, swissICT, swissprivacy.law, vsi.

[387] Et organisation : vsi.

[388] Canton : SO; parti : PVS; organisations : ASDPO, DigiGes.

que le responsable du traitement n'est pas tenu d'y réagir. Le canton de Thurgovie voudrait, au contraire, que les demandes de renseignement puissent uniquement se faire par écrit afin d'éviter des malentendus ou des conflits et pour empêcher une augmentation massive du nombre de demandes.

HDC note que le terme de « demande de renseignement » ne correspond pas à la notion utilisée dans la nLPD.

Al. 2

Plusieurs prestataires du domaine de la santé demandent que des précisions soient apportées au sujet des possibilités de communication des renseignements aux personnes ayant particulièrement besoin d'aide[389]. Un petit nombre de participants estiment que la consultation sur place devrait toujours pouvoir être possible, indépendamment de savoir qui l'a proposée[390]. La SPA estime qu'il faudrait préciser qu'en cas de consultation des renseignements sur place, le responsable remplit valablement son obligation, si, du fait d'un intérêt légitime, la communication de renseignements par écrit ne peut être raisonnablement exigée.

Il est écrit dans le rapport explicatif qu'en cas de consultation sur place, la personne concernée doit avoir la possibilité de demander une photocopie de certaines pièces de son dossier. Certains participants font remarquer que contrairement à ce qui figure dans le rapport, il n'existe pas de droit à la remise de dossiers ou de documents[391] ; en ce sens, le législateur a limité les informations aux « données personnelles traitées en tant que telles », ce qui permet de les communiquer sous forme agrégée. Cela devrait également être précisé dans le rapport explicatif[392]. FMH estime en revanche que la consultation sur place ne doit pas être une condition pour pouvoir recevoir une photocopie des documents : les personnes concernées devraient toujours pouvoir en recevoir une. swissICT relève qu'il est difficile de savoir quels types de documents peuvent être photocopiés en raison de l'expression « certaines pièces » utilisée dans le rapport explicatif. HÄRTING suggère de rédiger la disposition de manière à pouvoir rendre les photocopies payantes.

Al. 3.

Plusieurs participants remarquent que la formulation de l'al. 3 (les renseignements fournis doivent être « compréhensibles ») est trompeuse et peu claire puisqu'elle implique le recours à un critère subjectif basé sur les capacités de la personne concernée. Il faut se baser sur des critères plus objectifs[393]. Par exemple, il pourrait suffire de préciser que les données doivent être préparées et fournies sous une forme structurée, et donc compréhensible selon les règles de la bonne foi[394]. Toute exigence dépassant ce cadre ne serait plus proportionnée et entraînerait une charge de travail démesurée, qui ne permettrait dans certains cas plus de respecter le délai de 30 jours[395]. Cela aurait pour conséquence que les responsables devraient traiter davantage d'informations relatives à la personne concernée et que le droit d'ac-

[389] Organisations : ASPS, CURAVIVA, INSOS, IS, senesuisse, Spitex suisse.

[390] Organisations : ASDPO, swissprivacy.law.

[391] Organisations : ASSL, economiesuisse, Swiss Payment Association, swissICT, UPSA.

[392] Organisations : ASSL, economiesuisse, Swiss Payment Association, UPSA.

[393] Cantons : AR, AG, BE, BS, GL, NW, SH, SZ, UR, VD, ZH; organisations : Bär & Karrer, CFC, economiesuisse, FSA, IGEM, Préposé à la protection des données de SZ, OW et NW, privatim, proFonds, suva, SWICO, swissICT, Walderwyss.

[394] Organisations: ASB, eceonomiesuisse, suva, swissICT, VUD.

[395] Organisations : ASB, Economiesuisse, IGEM, suva, VUD.

cès ne pourrait plus s'intégrer aux processus standards des responsables du traitement[396]. La règlementation pourrait être mal comprise dans le sens où le responsable pourrait croire qu'il devra expliquer les informations qu'il fournit à la personne demandant les renseignements, voire les processus et les modèles commerciaux sous-jacents. Cette situation ouvrirait la porte à un allongement « artificiel » de la procédure, ne reposant pas sur un motif objectif, et à une augmentation de la charge de travail des responsables du traitement[397]. Il n'existe aucune base légale à ce sujet[398]. Au contraire l'art. 25, al. 2, nLPD dresse la liste des informations à fournir[399].

Pour ces raisons, il faudrait supprimer l'alinéa 3[400] ou définir des critères objectifs de compréhensibilité, par exemple en écrivant que les renseignements doivent être compréhensibles pour tous (« *allgemein verständlich* »)[401]. Une autre possibilité est de préciser que les renseignements doivent pouvoir être compris par la personne concernée dans la mesure de ses capacités cognitives / de son état cognitif (« *entsprechend den kognitiven Fähigkeiten/Zustands* »)[402], ou encore qu'elles doivent être compréhensibles sur le principe (« *im Grundsatz nachvollziehbar* »)[403]. De plus, quelques participants proposent d'ajouter une précision relative à la compréhensibilité des renseignements en écrivant qu'ils doivent être fournis dans une langue nationale ou en anglais[404]. Bär & Kärrer souhaite que l'on clarifie que le responsable doit uniquement fournir les renseignements mentionnés à l'art. 25, al. 1 et 2 nLPD.

Enfin, il s'agit d'un Swiss Finish aux yeux de Swico.

Al. 4

Quelques participants à la procédure de consultation estiment qu'il n'est pas nécessaire de mentionner à l'al. 4 qu'il faut protéger les données personnelles de tout accès de tiers non autorisé. Cette obligation découle de l'art. 8 nLPD ainsi que des dispositions du premier chapitre et de la section 1 du P-OLPD. Cet alinéa doit donc être biffé[405].

De plus, il manque une base légale pour soumettre la personne concernée à une réelle obligation de collaborer à son identification[406]. On propose de préciser que lorsqu'une personne ne collabore pas à son identification, le responsable peut refuser de lui fournir les renseignements[407].

Un dernier changement précis est demandé : celui de remplacer le terme d'« identification » par celui d'« authentification » (*Authentifizierung*)[408].

---

396 Cantons : AR, NW, SH, SZ, VD; organisations : Préposé à la protection des données de SZ, OW et NW, privatim.

397 Organisations : Economiesuisse, ASB.

398 Canton : ZH ; organisation : VUD.

399 Cantons: AG, BS, GL, SH, UR, ZH.

400 P. ex. cantons : VD, ZH.

401 Canton : BE.

402 Organisations : ASPS, CURAVIVA, INSOS, IS, senesuisse, Spitex suisse, usam.

403 Organisations : DFS, FSA, VUD.

404 Organisations : Curafutura, santésuisse.

405 Cantons : AG, AR, AI, GR, NW, OW, SH, SZ, VD, ZH; organisations : Préposé à la protection des données de SZ, OW et NW, privatim.

406 Organisations : IGEM, suva.

407 Organisations : IGEM, santésuisse, suva.

408 Organisations : IGEM, suva, VUD.

Al. 5

De nombreux participants affirment qu'il n'existe pas de base légale à l'obligation, figurant à l'al. 5, de documenter pourquoi la communication des informations est refusée, restreinte ou différée, et de conserver cette documentation[409]. Un petit nombre d'entre eux ajoutent qu'elle est contraire à la volonté du législateur[410]. En revanche, selon DigiGes, l'art. 8, al. 3, nLPD habilite le Conseil fédéral à édicter des dispositions définissant les exigences minimales en matière de sécurité des données personnelles ; l'al. 5 repose par conséquent sur une base légale. Quelques participants relèvent par ailleurs qu'il s'agit d'un Swiss Finish parce que le RGPD ne prévoit aucune obligation de conservation de ce type[411].

L'obligation de conserver la documentation de l'al. 5 a suscité beaucoup de critiques. L'art. 26, al. 4, nLPD prévoit déjà 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[412]. Une documentation sous la forme d'une copie de la réponse fournie à la personne concernée pourrait suffire à cet effet[413]. C'est en ce sens que le canton de Bâle-Ville note qu'il faudrait ajouter le critère de la forme écrite pour les renseignements, et supprimer le délai de conservation. Le canton de Glaris estime que les organes fédéraux doivent de toute façon inscrire les motifs de la restriction dans la décision. L'obligation de documentation et de conservation découle des obligations issues du droit procédural.

Selon certains, l'art. 20, al. 5, P-OLPD, basé sur l'art. 26, al. 4, nLPD génère du travail supplémentaire sans avoir de conséquences sur la possibilité pour la personne concernée de faire valoir son droit à l'information en justice si nécessaire[414]. De plus, à cause de cette réglementation, le responsable devrait traiter et conserver davantage de données personnelles qu'il n'en a besoin à des fins commerciales[415]. De ce fait, l'al. 5 est inutile dans la mesure où, en raison de la règle du fardeau de la preuve, le responsable du traitement a de toute façon un intérêt à pouvoir fournir une preuve du renseignement fourni[416].

Quelques participants à la procédure de consultation estiment qu'il est difficile de comprendre le besoin de conserver plus longtemps que les procès-verbaux de journalisation au sens de l'art. 3 P-OLPD la documentation relative au refus, à la restriction ou au report de la communication des informations. De concert avec d'autres participants, ils considèrent que le délai devrait être raccourci[417]. DigiGes souligne toutefois l'importance de cette norme pour que les personnes concernées puissent faire valoir leurs droits. Cette réglementation émane du prin-

[409] Canton : LU; parti : Le Centre; organisations : ASB, ASP, ASSL, Association de commerce, BNS, Bär & Karrer, Creditreform, Datenschutzguide.ch, economiesuisse, EPS, EXPERTsuisse, FSA, FSEP, H+, IGEM, Migros, pharmasuisse, Ringier, Scienceindustries, SPA, suisa, SwissHoldings, swissICT, swissprivacy.law, swissstaffing, UPSA, usam, UVS, vsi, VUD, Walderwyss.

[410] Organisations : ASB, FSA, Pharmasuisse, UVS.

[411] Organisations : ASSL, economiesuisse, Migros, Scienceindustries, SwissHoldings, UPSA.

[412] Cantons: AG, AR, NW, SH, SZ, VD, ZH; organisations: Préposé à la protection des données de SZ, OW et NW, privatim, Ringier, SPA.

[413] Organisations: BNS, H+, IGEM, swissICT, VUD.

[414] Cantons : AG, AR, BL, GR, NW, OW, SH, SZ, VD, ZH ; organisations : H+, IGEM, Préposé à la protection des données de SZ, OW et NW, privatim, Ringier, VUD.

[415] P. ex. organisation : BNS.

[416] Organisations : Economiesuisse, Migros, Scienceindustries, SPA, Walderwyss.

[417] Organisations : ASA, ASP, Bär & Karrer, curafutura, EPS, FER, FMH, FSEP, proFonds, Ringier, SWICO, vsi.

cipe de la transparence. C'est pourquoi certains demandent que le délai de conservation obligatoire soit prolongé à cinq ans[418]. Cette durée correspond au délai de prescription d'un grand nombre de créances[419].

Enfin, de l'avis de certains, la terminologie (« informations » et « renseignements ») gagnerait à être uniformisée[420].

3.2.21 Art. 21 P-OLPD : Responsabilité

Selon economiesuisse, les deux alinéas de l'art. 21 visent le traitement coordonné des demandes de renseignements par plusieurs responsables du traitement, sans que cela ne soit suffisamment clair[421]. Dans le même ordre d'idées, certains participants regrettent la formulation peu claire de l'article. Si l'on optait ici pour une réglementation réglant davantage que les questions de coordination, on ne sait pas quelles seraient les conséquences juridiques d'une absence de responsabilité[422]. ASDPO, qui considère aussi que cet article porte sur la coordination regrette qu'aucune disposition ne règle la question générale des responsabilités entre responsables conjoints du traitement à l'instar de l'art. 26 RGPD.

Al. 1

En ce qui concerne l'al. 1, de nombreux participants souhaitent une clarification quant au fait que la responsabilité est conjointe[423]. En ce qui concerne les autorités fédérales, ils signalent que l'obligation de transmettre constitue de toute façon un principe de droit administratif qui découle du lien de souveraineté entre l'État et les citoyens[424]. Les critiques formulées divergent cependant en ce qui concerne les responsables privés. Plusieurs participants estiment qu'imposer une telle obligation aux personnes privées serait disproportionné. Les parties déterminent leurs droits et obligations de manière autonome lorsque la relation se fonde sur du droit privé. L'obligation de transmettre la demande engendre une charge de travail supplémentaire pour les responsables du traitement privés sans toutefois permettre de renforcer les droits des personnes concernées[425]. En revanche, FRC salue le fait que la personne concernée ait la possibilité d'adresser sa demande auprès de chaque responsable de traitement. Cela renforce ses droits.

Outre cet aspect, des critiques générales ont été formulées. En pratique, un responsable du traitement ne sait pas toujours si d'autres responsables peuvent également être compétents, ni qui ils sont. De ce fait, il n'est souvent pas en mesure de satisfaire à la demande[426]. Transmettre la demande en cas d'incertitude nuirait par ailleurs à la protection des données[427]. D'après certains, il convient de préciser la première phrase en écrivant qu'elle porte uniquement sur les données pour lesquelles plusieurs responsables sont conjointement compétents[428]. Le Centre ajoute qu'avec la tournure actuelle, un responsable pourrait, à sa seule

[418] Organisations : ASDPO, DFS, Swimag.

[419] Organisation: Swimag.

[420] Organisations : ASDPO, swissprivacy.law.

[421] Organisations : ASB, Economiesuisse.

[422] Organisations : IGEM, santésuisse, suva, VUD.

[423] Organisations : ASB, Bär & Karrer, DFS, FSA, IGEM, suva, VUD.

[424] Cantons : AG, AR, BS, GL, SH, SO, UR, VD, ZH; organisation : privatim.

[425] Cantons : AG, AR, BS, SH, SO, VD, ZH; organisation : privatim.

[426] Parti : Le Centre; organisations : economiesuisse, ASB.

[427] Organisations : ASB, Economiesuisse.

[428] Organisation: ASB.

discrétion, rejeter la responsabilité et transmettre une demande de renseignements à un sous-traitant de manière infondée.

ASB fait enfin remarquer que des difficultés pourraient survenir si le responsable du traitement est domicilié à l'étranger, notamment parce qu'il est interdit de transférer des demandes de renseignements dans des courriels non sécurisés.

Al. 2

ASB estime que le deuxième alinéa n'est pas pertinent du fait que le cas du sous-traitant peut être subordonné à l'al. 1. Les alinéas portent tous deux sur le traitement coordonné des demandes de renseignement.

Certains participants à la consultation considèrent cet alinéa comme problématique et estiment que transférer l'obligation de renseigner du responsable au sous-traitant ébranle les règles relatives aux compétences établies à l'art. 25, al. 4, nLPD. Selon eux, l'al. 2 doit être biffé[429]. Le responsable a pour tâche de recueillir les informations nécessaires à la communication de renseignements auprès du sous-traitant et de se prononcer sur la demande de renseignements[430].

Selon quelques participants, l'al. 2 prévoit la possibilité pour le responsable de ne pas transmettre la demande sans y répondre, alors qu'il devrait être en mesure d'y répondre[431]. Le Centre regrette aussi que cette formulation puisse permettre à un responsable de rejeter la responsabilité à sa seule discrétion et sans justification, et qu'il transmette la demande de renseignements à un sous-traitant. SWICO relève en revanche qu'en vue d'assurer la conformité, un responsable du traitement ne peut pas se permettre de simplement transférer les demandes de renseignements au lieu de mettre sur pied les processus internes nécessaires.

economiesuisse suggère qu'il vaudrait mieux obliger le sous-traitant à soutenir le responsable du traitement en matière de communication des renseignements[432]. Les sous-traitants ne peuvent pas souvent répondre aux demandes, voire ils ont l'obligation contractuelle de ne pas le faire[433].

3.2.22 Art. 22 P-OLPD : Délais

Al. 1

Les participants sont très nombreux à noter que le délai devrait seulement courir à partir du moment où la demande est claire et que la personne concernée a été correctement identifiée[434]. Selon eux, il faut que la demande respecte les exigences formelles[435]. DigiGes souligne toutefois qu'il ne faudrait pas lier le délai à une condition parce que cela laisserait une trop grande marge de manœuvre aux responsables, ce qui pourrait considérablement limiter les droits de la personne concernée. Le canton de Soleure souhaite que la disposition de

[429] Cantons : SG; organisations : FSA, HÄRTING, swissICT.

[430] Cantons : GL, SG; organisations : HÄRTING, SWICO.

[431] Organisations : ASB, Economiesuisse, IGEM, santésuisse, suva, VUD.

[432] Et organisation: SWICO.

[433] Organisations : ASB, Economiesuisse, VUD.

[434] Organisations : ASB, ASP, ASSL, auto suisse, Creditreform, economiesuisse, EPS, FSA, FSEP, IGEM, Ringier, santésuisse, SPA, suva, Swiss Insights, swissprivacy.law, UPSA, usam, vsi, VUD, Walderwyss.

[435] Organisations : ASP, Creditreform, EPS, FSEP, swissprivacy.law, usam, vsi.

l'ordonnance fasse clairement ressortir que les renseignements doivent être fournis dans les 30 jours, comme l'exige l'art. 25, al. 7, nLPD.

En outre, certains veulent que les féries judiciaires soient prises en compte car beaucoup de personnel est absent durant cette période[436].

Al. 2

Le canton de Soleure écrit que la disposition devrait clairement indiquer que les réponses aux demandes de renseignements après 30 jours doivent rester l'exception. Dans cette optique, certains participants à la procédure de consultation souhaitent compléter la disposition par un délai maximal afin de limiter la marge de manœuvre des responsables du traitement et d'éviter que le délai soit prolongé indéfiniment. Cela protégerait en outre les droits de la personne concernée[437].

L'ASDPO propose que cet al. 2 porte aussi sur la communication d'un refus, d'une restriction ou d'un report du droit d'accès.

Swimag suggère que le délai pour fournir des renseignements soit réduit à trois jours lorsque la personne concernée accepte l'échange de données sous format électronique et qu'elle fournit une demande de renseignements signée au moyen d'une signature électronique qualifiée et certifiée selon la loi fédérale du 18 mars 2016 sur la signature électronique[438] et l'art. 14 CO, ou sur présentation d'une E-ID en incluant une note mentionnant l'urgence de la situation. Sa suggestion est en adéquation avec les conditions de vie modernes.

3.2.23 Art. 23 P-OLPD : Exceptions à la gratuité

Al. 1

Dans le rapport explicatif au moins, les participants souhaitent que l'expression d'« efforts disproportionnés » soit précisée. Cette précision est particulièrement importante parce que le fait de mettre les frais à la charge de la personne entrave ses droits d'accès[439].

SWICO estime que la disposition devrait explicitement s'appliquer aux demandes de renseignements introduites de manière procédurière[440].

Al. 2

Plusieurs participants à la procédure de consultation soulignent qu'une participation aux frais doit rester une exception ou plaident en faveur de la gratuité permanente des renseignements[441]. La participation aux frais ne doit pas devenir un moyen pour les responsables du traitement dissuadent les personnes concernées d'avoir accès à leurs données. Pour cette raison, elle ne devrait être autorisée qu'« à titre exceptionnel »[442]. DigiGes relève qu'il existe

[436] Organisations : ASPS, CURAVIVA, INSOS, IS, senesuisse, Spitex suisse.

[437] Organisations: DigiGes, FRC, PVS, Stiftung für Konsumentenschutz, swissICT.

[438] SCSE ; RS **943.03**.

[439] Cantons : GE, SG; organisations : Association de commerce, swissICT.

[440] Et organisation: ASA.

[441] Partis: PVS, PS; organisations : DigiGes, FRC, Stiftung für Konsumentenschutz.

[442] Organisation: FRC.

déjà une exception à la gratuité, et qu'elle est fréquemment utilisée pour étendre les possibilités de contrer les demandes de renseignements. Par conséquent, il faut absolument supprimer cette exception. D'autres participants demandent la gratuité indépendamment de la charge de travail engendrée, parce que le responsable du traitement doit disposer d'un système qui permette d'accéder facilement aux données traitées en vertu du principe de « *privacy by design* ». Si les responsables se retrouvaient face à une charge de travail « disproportionnée » car leur système est inadapté, ils ne pourraient pas mettre les frais à la charge de la personne concernée[443]. PS demande que le plafond des coûts ne soit au moins pas augmenté.

Stiftung für Konsumentenschutz plaide pour que la personne concernée doive uniquement participer aux frais lorsque la demande de renseignements est objectivement procédurière. Quelques autres participants considèrent quant à eux que ces demandes devraient elles aussi être traitées sans frais, faute de quoi la disposition pourrait être interprétée de manière abusive[444]. Le canton de Thurgovie souhaite que l'art. 2, al. 1, let. a, de l'OLPD en vigueur soit repris de manière à ce que la participation aux frais puisse être demandée lorsque les renseignements désirés ont déjà été communiqués à la personne dans les 12 mois précédant la demande, et que cette dernière ne peut plus justifier d'un intérêt légitime.

Selon PPS, une distinction devrait être faite entre les entreprises dont le traitement des données personnelles est de nature purement administrative, et les entreprises dont le modèle économique est basé sur la collecte, l'analyse, la mise à disposition et/ou l'utilisation de données personnelles.

FRC souhaite qu'en plus de chiffrer les coûts extraordinaires, le responsable du traitement doive expliquer ce qui les justifie.

À l'opposé des avis mentionnés précédemment, plusieurs participants trouvent que la limite de 300 CHF est trop basse et qu'elle devrait être relevée. Cette somme est insuffisante par rapport à la charge de travail requise pour répondre aux demandes de renseignements[445]. Santésuisse ajoute que le nombre de demandes générales a fortement augmenté au cours des dernières années. La quantité de données qui doivent être fournies a également augmenté. Le canton de Soleure relève que dans certains cas exceptionnels, les demandes peuvent générer une charge de travail supplémentaire considérable pour les responsables du traitement. VUD souligne quant à lui que le montant de la participation devrait avoir un effet dissuasif afin que les personnes concernées n'exigent des renseignements lorsque cela s'avère nécessaire[446].

[443] Partis : PVS, PPS; organisations : DigiGes, Swimag.

[444] Parti : PVS; organisations : DigiGes, Swimag: wünscht eine Legaldefinition des Querulanten.

[445] Cantons : SO (500 CHF), GE; partis : Le Centre, organisations : UPSA, IS (1000 CHF), ASPS (1000 CHF), auto suisse, Creditreform (1000 CHF), curafutura, CURAVIVA (1000 CHF), economiesuisse, Gastrosuisse, Association de commerce, HÄRTING, IGEM (3000 CHF), INSOS (1000 CHF), EPS (1000 CHF), ASP (1000 CHF), santésuisse (2000 CHF), ASB, senesuisse (1000 CHF), usam (1000 CHF), ASSL (5000 CHF), SPA, Spitex (1000 CHF), suva (3000 CHF), ASA, swissstaffing (1000 CHF), vsi, FSEP (1000 CHF), VUD (mindestens 3000 CHF), Walderwyss (5000 CHF).

[446] Organisations : IGEM, suva, VUD.

Un petit nombre de participants fait remarquer que le RGPD ne pose pas de limite : il exige uniquement le paiement de frais « raisonnables »[447]. Le canton de Genève propose d'harmoniser le montant exigé avec celui figurant dans l'initiative parlementaire sur le principe de la transparence dans l'administration, c'est-à-dire de fixer un plafond de 2000 CHF[448].

Al. 3

Pour plusieurs participants, la personne concernée devrait explicitement confirmer qu'elle accepte la participation aux frais. Une absence de réponse ne devrait en aucun cas pouvoir être interprétée comme un consentement aux frais[449]. Ainsi, le responsable du traitement n'aurait pas à déployer des efforts disproportionnés sans obtenir de garantie quant au paiement[450]. De plus, cette précision améliorerait la sécurité juridique des personnes concernées[451], qui devraient, le cas échéant, payer au maximum 300 CHF[452]. Le canton de Vaud ajoute que cette disposition pourrait être complétée par un renvoi aux dispositions topiques de la législation sur la protection des données qui régissent la procédure à suivre lorsque la personne concernée conteste l'émolument demandé.

En tenant compte du fait que les renseignements doivent être fournis dans les 30 jours, la FER considère que le délai de 10 jours paraît long, et qu'il devrait être raccourci à 7 jours. D'autres participants pensent que le début du délai doit être précisé ou que le délai de réponse de 30 jours ne doit commencer à courir qu'après les dix jours de réflexion ou, le cas échéant, après la confirmation de l'acceptation des frais, afin que le délai ne se retrouve pas réduit à 20 jours dans les faits[453].

3.2.24 Art. 24 P-OLPD : Droit à la remise ou à la transmission des données personnelles (portabilité des données)

La première remarque concernant le commentaire de l'art. 24 P-OLPD est que le terme de « portabilité des données » n'a été introduit qu'à partir des débats parlementaires au sujet de la révision de la LPD. Le message relatif à la nLPD ne contient de ce fait pas d'explication à ce sujet[454]. Il ne suffit donc pas que l'art. 24 P-OLPD renvoie aux dispositions relatives au droit d'accès. En lieu et place de cela, établir une réglementation détaillée s'impose[455]. Certains participants soulignent que la portabilité des données est un acquis majeur, alors que le monde numérique est malheureusement de plus en plus souvent divisé en silos de données. Le PVS considère qu'une réglementation détaillée est importante[456].

Bär & Karrer estime que la personne concernée poursuit un autre but lorsqu'elle exerce son droit à la remise ou à la transmission des données personnelles que lorsqu'il s'agit de son droit d'accès. Les effets « *lock in* » (clientèle captive) peuvent uniquement être contrés si les personnes concernées ont la possibilité de recevoir les données dans un format structuré, accessible et lisible par une machine. C'est pourquoi le fait que le responsable remette les

[447] Organisations : IGEM, suva, VUD.

[448] https://www.parlament.ch/centers/documents/fr/bericht-spk-n-16-432-2020-10-15-f.pdf.

[449] Organisations : ASDPO, FRC, santésuisse, Stiftung für Konsumentenschutz, swissprivacy.law.

[450] Organisations : HTC, santésuisse, swissprivacy.law.

[451] Organisation: Santésuisse.

[452] Organisation: Stiftung für Konsumentenschutz.

[453] Organisations : ASB, ASDPO, economiesuisse, FSA, HDC, HÄRTING, IGEM, SPA, swissICT, swissprivacy.law, VUD.

[454] Organisations : ASSL, auto suisse, SPA, Swiss Insights, UPSA, usam.

[455] Cantons : AG, AR, SH, VD, ZH; organisations : auto suisse, privatim, PVS, SPA, Swiss Insights, usam.

[456] Parti : PVS; organisations : Bär & Karrer.

données dans un format précis est un aspect décisif du droit à la remise ou à la transmission des données personnelles. En revanche, le format n'a pas d'importance lorsqu'il s'agit du droit d'accès.

Il faudrait par exemple définir concrètement ce que sont les « formats électroniques couramment utilisés » (art. 28, al. 1, nLPD). Il serait également pertinent de régler la question des « efforts disproportionnés » (art. 28, al. 2, nLPD) exigés pour la transmission directe d'un responsable du traitement à un autre. En outre, en ce qui concerne les exceptions à la gratuité, une réglementation différente de celle du droit d'accès serait concevable, car ce n'est ici pas la protection de la personnalité mais la valeur économique des données qui est au premier plan[457]. swiss ICT ajoute que l'art. 24 P-OLPD ne devrait pas renvoyer à l'art. 22 P-OLPD (délais) car il y a contradiction entre ces deux articles. Swimag estime que l'art. 24 devrait renvoyer à l'art. 20 dans son ensemble, mais pas l'art. 23 P-OLPD.

Quelques participants à la procédure de consultation considèrent que le droit à la portabilité des données ne peut pas être absolu[458]. Il ne faut en aucun cas qu'il engendre une obligation d'utiliser des systèmes de traitement des données standards[459]. Ce droit ne peut exister que si le traitement des données personnelles peut être opéré dans un format couramment utilisé[460]. C'est une précision qu'il convient d'ajouter dans l'ordonnance, selon l'usam. Certains autres participants exigent même qu'il n'y ait pas d'obligation pour le responsable d'utiliser un système de traitement des données compatible sur le plan technique[461].

En substance, HDC ajoute ce qui suit : puisque l'art. 28 nLPD est repris du RGPD, dont la logique est différente, les données traitées sans atteinte à la personnalité au sens de l'art. 30 nLPD (et donc sans consentement ou contrat) ne peuvent pas faire l'objet d'un droit à la remise.

3.2.25 Art. 25 P-OLPD : Conseiller à la protection des données

Al. 1

Plusieurs participants approuvent explicitement la disposition du projet[462]. D'autres se montrent davantage critiques : par exemple, selon des cantons, l'art. 25 P-OLPD ne se réfère pas suffisamment à l'art. 10, al. 2, nLPD[463], mais il se contente de reprendre le contenu de l'ordonnance en vigueur[464]. L'art. 10, al. 2, nLPD prévoit que le conseiller à la protection des données forme et conseille les responsables du traitement et qu'il concoure à l'application des prescriptions relatives à la protection des données : ainsi, les tâches décrites à l'art. 25 ne sont pas les tâches que le conseiller doit remplir, mais seulement une concrétisation partielle des obligations énoncées dans la loi. Cela devrait être précisé à l'art. 25 P-OLPD[465].

[457] Cantons : AG, AR, SH, VD, ZH; Organisation : privatim.

[458] Organisations : ASP, Creditreform, EPS, FSEP, usam, vsi.

[459] Organisations : ASSL, auto suisse, Swiss Insights, UPSA.

[460] Organisations : ASP, Creditreform, EPS, FSEP, usam, vsi.

[461] Organisations : ASSL, auto suisse, Swiss Insights, UPSA, usam : toutes le précisent dans la proposition concrète de reformulation.

[462] Organisations : ASPS, CURAVIVA, INSOS, IS, senesuisse, Spitex suisse.

[463] Cantons : AI, AG, AR, GR, NW, SH, SZ, UR, VD, ZH; organisations : Préposé à la protection des données de SZ, OW et NW, privatim.

[464] Organisation: SWICO.

[465] Cantons : AG, AR, GR, NW, SH, SZ, UR, VD, ZH; organisations : Bär & Karrer, Préposé à la protection des données de SZ, OW et NW, privatim, SPA. Bär & Karrer souhaite qu'il soit précisé si les tâches énumérées sont exhaustives ou non.

Trois cantons suggèrent par exemple d'ajouter « en particulier »[466]. D'autres participants souhaitent que l'on conserve uniquement l'art. 10, al. 2, nLPD parce qu'il est suffisamment détaillé[467]. Le DFS recommande de préciser les tâches du conseiller à la protection des données, dont la description actuelle est trop rudimentaire. En plus du concours à l'établissement de l'analyse d'impact relative à la protection des données, cet alinéa devrait évoquer les tâches du conseiller ayant trait au renforcement de la protection des données. Il devrait par exemple agir davantage de manière préventive[468]. L'ASDPO demande quant à elle l'ajout d'un inventaire des tâches ou une description de la fonction du conseiller.

Une remarque conceptuelle de nature linguistique a été faite concernant l'allemand : il n'est dans ce contexte pas exact d'utiliser le verbe « *wahrnehmen* » ; il faudrait à la place utiliser « *haben* » (conceptuellement, il n'est pas correct de dire que le conseiller doit « accomplir » certaines tâches, mais il faudrait écrire que ses tâches « sont » les suivantes) [469].

D'après SWICO, les tâches sont décrites comme étant des obligations légales personnelles du conseiller à la protection des données, ce qui soulève des questions en matière de responsabilité auxquelles l'article ne répond pas. Des adaptations ou des clarifications doivent être apportées. De plus, d'autres participants estiment que la formulation de la disposition devrait être impérative parce que les responsables privés sont libres de recourir à un conseiller à la protection des données ou non. Si cette disposition vise à exprimer que les responsables privés sont également obligés d'avoir un conseiller à la protection des données, il manque la base légale nécessaire[470].

La SPA relève que la distinction entre le conseiller à la protection des données et le responsable du traitement n'est pas claire lorsqu'une entreprise a désigné un délégué à la protection des données au sens de l'art. 37 RGPD.

Let. a

Plusieurs participants soulignent que l'art. 10, al. 2, nLPD n'exige pas de mettre sur pied un contrôle général de tous les traitements de données personnelles, même si la let. a de l'art. 25 P-OLPD le prévoit[471]. L'obligation de contrôler tous les traitements de données est par ailleurs contraire à l'approche basée sur le risque prévue à l'art. 8 nLPD. Le fait que le rapport explicatif sous-entende qu'il faut contrôler tous les traitements est incorrect : le contrôle devrait s'effectuer selon une approche basée sur le risque[472].

Difficile donc de savoir dans quelle mesure les traitements doivent être contrôlés (tous, certains, seulement ceux soumis au conseiller, ceux qui ont été sélectionnés en fonction du risque, etc.)[473]. Economiesuisse estime que seul un devoir de consultation existe et qu'en dehors de celui-ci, les conseillers n'ont qu'une fonction générale de conseil. L'obligation de con-

[466] Cantons : NW, OW, SZ.

[467] Canton : BS; organisation : FSA.

[468] Organisations : ASDPO, DFS.

[469] Organisations : ASB, IGEM, suva, VUD.

[470] Cantons : LU; organisations : ASDPO, SPA.

[471] Cantons : BS, SG; organisations : ASA, Curafutura.

[472] Cantons : LU; organisations : ASA, IGEM, suva, VUD.

[473] Organisations : ASB, economiesuisse, IGEM, la Poste, les banques domestiques, suva, VUD.

trôler fixée à l'al. 1, let. a devrait par conséquent se limiter aux traitements qui sont « soumis » au conseiller[474]. HÄRTING affirme en revanche que le législateur a explicitement prévu, contrairement à ce qui figure dans le RGPD, que les conseillers doivent aussi être garants de la protection des données et qu'ils peuvent et doivent intervenir eux-mêmes, et ne pas seulement assumer une fonction de vérification de la conformité et de contrôle. Selon la VUD, on ne sait pas ce que cela impliquerait si le conseiller ne remplit pas le devoir de contrôle étendu[475].

Pour le canton de Bâle-Ville, un devoir de contrôle si étendu est disproportionné. Il rate sa cible en transformant les conseillers en « policiers ». Il faudrait plutôt mettre l'accent sur leur fonction de conseil, surtout lorsque les organes responsables souhaitent faire appel aux conseillers[476]. Du simple fait du nombre de traitements opérés, des participants affirment qu'il serait impossible de tous les contrôler en pratique. Le conseiller ne pourrait pas non plus avoir connaissance de tous les traitements qui méritent d'être contrôlés[477]. Un autre aspect critiqué est que le contrôle supplémentaire du traitement de données personnelles et de l'analyse d'impact conduirait, dans les faits, à transférer la responsabilité aux conseillers à la protection des données. Le texte devrait exclure cette possibilité[478].

Par souci du détail, Santésuisse relève que l'ajout de l'expression « ainsi que ses exigences » n'était pas nécessaire, puisque l'examen des exigences fait déjà partie du contrôle.

Let. b

L'al. 1, let. b est également contraire, pour certains, à la fonction de conseil[479] et à la liberté d'organisation des responsables qui fixent les obligations en tenant compte de la situation concrète de l'entreprise[480]. Une atteinte d'une telle ampleur à l'autonomie privée aurait dû être prévue par la loi[481]. D'autre part, il a été relevé que cette lettre est superflue et répétitive en raison de la règle particulière figurant dans la norme supérieure (art. 24, al. 4, nLPD)[482].

La let. b est en outre contraire à de nombreuses réglementations sectorielles[483]. Elle contrevient au modèle international établi des trois lignes de maîtrise (*three lines of defense model)*[484]*.*

IGEM note que la seule présentation de l'analyse d'impact au conseiller ne suffit pas et qu'il doit participer à son établissement. Pour ce faire, il doit vérifier l'évaluation des risques et les mesures proposées[485].

[474] Ebenso organisations : ASB, la Poste, swissICT (du même avis).

[475] Ebenso organisations : IGEM, suva.

[476] Organisations : IGEM, suva, swissICT (du même avis), UBCS, VUD.

[477] Organisations : ASB, La Poste, UBCS.

[478] Canton : SG; organisation : Curafutura.

[479] Organisations : ASB, economiesuisse, la Poste, swissICT (du même avis), UBCS.

[480] Organisations : ASA, ASB, economiesuisse, la Poste.

[481] Organisations : ASB, economiesuisse, la Poste, swissICT (du même avis).

[482] Organisations : ASB, HÄRTING.

[483] Organisations : ASB, la Poste, swissICT (du même avis), UBCS.

[484] Organisations : ASB, Econmiesuisse, swissICT (du même avis).

[485] Et organisation: Suva.

Un petit nombre de participants à la procédure de consultation demandent un ajout qui devrait permettre que dans les cas graves, le conseiller puisse informer les « *die höchsten Organe [der jeweiligen Privaten oder Bundesorgane]* »(les plus hautes instances [privées ou fédérales])[486].

Al. 2

Economiesuisse relève que la let. b prévoit à juste titre un droit d'intervention. Il serait toutefois souhaitable de compléter le droit d'intervention de la let. b par un droit à demander l'avis d'une autorité supérieure dans une nouvelle let. c (« *Eskalationsrecht* »). Cela est nécessaire pour que le conseiller à la protection des données ne doive pas uniquement s'appuyer sur les documents qui sont à sa disposition pour procéder aux contrôles internes à l'entreprise quant au respect des règles de protection des données, mais qu'il puisse aussi se procurer des informations et des documents supplémentaires[487].

Cela crée une réglementation qui permet aux conseillers à la protection des données, en cas de situation complexe ou d'infractions particulièrement graves aux règles de protection des données, de pouvoir être entendu à un plus haut niveau hiérarchique et de pouvoir obtenir une décision. Il aurait aussi la possibilité de recourir à une organisation responsable de la conformité ou de remonter la voie hiérarchique, en accord avec celle-ci. Sans ce type de norme, les conseillers à la protection des données s'exposeraient au risque d'être eux-mêmes tenus pour responsables[488]. Selon l'ASDPO il faudrait dans tous les cas que l'on précise à l'art. 25 P-OLPD quelle est la responsabilité (civile, pénale) du conseiller.

Santésuisse fait remarquer que pour les conseillers à la protection des données des personnes privées, il manque une norme analogue à l'art. 28 P-OLPD, qui consacrerait l'indépendance du conseiller et le fait qu'il ne doit pas recevoir d'instructions.

3.2.26 Art. 26 P-OLPD : Exception à l'obligation de tenir un registre des activités de traitement

Sur le principe, les participants approuvent l'exception[489]. La limite de 250 collaborateurs est basée sur le droit des sociétés anonymes[490]. Le CP estime que la grande majorité des PME devrait pouvoir bénéficier de cette exception, qui est par ailleurs conforme à l'approche fondée sur le risque adoptée dans la nLPD. Des participants issus de l'économie privée souhaitent même un assouplissement supplémentaire, ou une précision, afin de réduire les charges pesant sur les petites entreprises. Spitex écrit que l'exception prévue ne s'appliquerait pas à de nombreuses entreprises parce qu'elles traitent des données sensibles à grande échelle ou qu'elles font partie d'un groupe qui emploie, dans son ensemble, plus de 250 collaborateurs[491]. Plusieurs veulent que le critère utilisé soit celui d'une moyenne de 250 équivalents plein-temps par année et non pas celui du nombre de collaborateurs[492].

[486] Organisations : Economiesuisse, ASB, VUD.

[487] Et organisation: ASB.

[488] Organisations : ASB, Economiesuisse.

[489] Cantons : LU; organisations : ASPS, CP, CURAVIVA, HDC, INSOS, IS, proFonds, senesuisse, Spitex suisse, SwissFoundations.

[490] P. ex. pour les exceptions au contrôle ordinaire au sens de l'art. 727, al. 2, CO.

[491] Et organisations : ASPS, CURAVIVA, INSOS, IS, senesuisse.

[492] Organisations : FSA, ProFonds (si, en moyenne annuelle, une association ou une fondation emploie plus de 250 équivalents temps-plein deux ans d'affilée, elle devrait se soumettre à un contrôle ordinaire au sens de l'art. 727 CO), swissICT, VUD.

Beaucoup sont cependant critiques quant au fait que les critères définissant le traitement de données sensibles à grande échelle ou le profilage à risque élevé ne couvrent de loin pas tous les traitements présentant un risque pour les droits de la personnalité. Ici aussi, comme dans le cas de l'art. 4, al. 1, P-OLPD, il convient de reprendre les exigences relatives à l'analyse d'impact sur la protection des données[493]. La FRC ajoute qu'il est bienvenu de vouloir limiter l'exception, mais que ce principe risque d'être vidé de toute portée si les notions de « données sensibles à grande échelle » et de « profilage à risque élevé » ne sont pas mieux définies. La question se pose même de savoir si le fait de traiter de données sensibles ne devrait pas, en soi, constituer une exception sans qu'il soit nécessaire d'être face à un traitement à grande échelle. L'ASDPO souhaite que l'on s'inspire davantage de l'art. 30, al. 5, RGPD. Ces participants regrettent beaucoup le fait qu'il existe une exception pour les entreprises de moins de 250 employés[494]. L'instrument du registre des activités de traitement perd trop facilement de son utilité[495]. La tenue d'un registre constitue un moyen simple pour permettre au responsable du traitement de s'assurer qu'il respecte ses obligations en matière de protection des données[496]. Il s'agit par ailleurs d'un exercice indispensable à la bonne gouvernance de la protection et de la sécurité des données[497]. La tenue d'un registre avec les outils modernes ne représente par ailleurs pas une charge de travail significativement lourde, même pour les entreprises individuelles. Le registre sert toutefois à la sensibilisation et à l'amélioration de leur protection[498]. Pour les PME en particulier, il s'agit d'un point crucial car elles traitent un volume de données personnelles toujours plus important et comptent par conséquent parmi les cibles privilégiées des hackers[499].

L'ASB estime que la tournure utilisée impliquerait qu'il faille tenir un registre pour toutes les activités de traitement à partir du moment où les conditions de l'exception ne sont pas remplies. Certains aimeraient que l'on précise si c'est effectivement ce qui est prévu ou non[500]. D'autres partent du principe que la disposition ne pourrait pas être interprétée de la sorte et souhaitent que l'on limite l'obligation de tenir un registre aux traitements qui remplissent les conditions[501]. On tiendrait ainsi suffisamment compte à la fois de la protection des personnes concernées et des besoins des PME[502]. EXPERTsuisse souhaite une clarification des conséquences d'une mauvaise tenue du registre.

Selon plusieurs participants l'art. 12, al. 5, nLPD ne permet une exception à l'obligation de tenir un registre des activités de traitement que lorsque l'on est en présence d'un « risque limité ». Il faut donc en conclure qu'en soi, le risque est limité dès lors que les conditions de la let. a et celles de la let. b ne sont pas remplies[503]. Cela restreint fortement le champ d'application de l'analyse d'impact relative à la protection des données au sens de l'art. 22 nLPD[504].

---

493 Cantons : AG, AR, GR, NW, SH, SO, SZ, VD, ZH; partis : PVS; organisations : ASDPO, Préposé à la protection des données de SZ, OW et NW, privatim.

494 Organisations : ASDPO, FRC.

495 A titre d'exemple, on mentionne la constitution d'une filiale qui serait uniquement affectée au traitement des données sensibles à grande échelle ou au profilage.

496 Organisations : ASDPO, FRC.

497 Organisation : ASDPO.

498 Organisation : Swimag.

499 Organisation : FRC.

500 Organisations : EXPERTsuisse, FSA, SWICO.

501 Parti : Le Centre; organisations : ASB, ASSL, auto suisse, economiesuisse, FSA, HDC, IGEM, santésuisse, Scienceindustries, suva, Swiss Insights, UPSA, usam, VUD.

502 Organisations : ASSL, auto suisse, economiesuisse, Swiss Insights, UPSA.

503 Organisations : ASB, ASSL, auto suisse, economiesuisse, IGEM, suva, Swiss Insights, UPSA, VUD.

504 Organisations : ASB, IGEM, suva, VUD.

D'autres participants estiment que la disposition n'est pas claire : seuls les deux cas énoncés présenteraient-ils un risque élevé ? Ils souhaitent que l'on précise s'il s'agit d'une liste exhaustive ou non[505]. Ils veulent par ailleurs savoir si les critères des let. a et b sont également ceux qui permettent de définir si une analyse d'impact doit être effectuée ou s'ils s'appliquent à l'obligation d'annoncer les violations de la sécurité des données selon l'art. 24 nLPD[506]. Enfin, certains font remarquer que l'exception ne s'applique aux art. 3 (journalisation) et 4 (règlement de traitement des personnes privées) P-OLPD, mais uniquement au registre des activités de traitement, ce qui est d'une certaine façon absurde[507].

Les CFF souhaitent que les entreprises de transport restent libérées de l'obligation de déclarer leur registre d'activités de traitement au PFPDT comme prévu à l'art. 12, al. 4, nLPD si elles désignent un conseiller à la protection des données.

Let. a

La notion de traitement portant sur données sensibles à grande échelle en particulier n'est pas suffisamment précise aux yeux des participants, et elle laisse une trop grande marge d'interprétation. Le terme de traitement « à grande échelle » doit être précisé[508]. La FRC elle aussi estime que ces notions devraient être mieux définies pour ne pas vider de toute portée la disposition.

Les milieux économiques proposent à titre d'exemple de préciser la notion en fixant une limite d'au moins 1000 jeux de données (« *1000 Datensätze* »)[509]. De manière plus générale, l'UPSV est en faveur d'une définition stricte qui s'appuierait par exemple sur le rapport entre l'ensemble des données personnelles et les données sensibles. En revanche, le PS et l'USS estiment que la notion de traitement à grande échelle ne devrait pas être trop restrictive.

Let. b

Pour davantage de clarté, le canton de Lucerne souhaiterait ajouter au critère du profilage qu'il présente un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

D'une manière générale, il faudrait prévoir des délais transitoires pour l'obligation de tenir des registres parce qu'ils nécessitent une charge de travail très élevée[510]. En outre, il est demandé de préciser que les registres peuvent non seulement être tenus sous forme écrite, mais aussi sous une autre forme qui permet la preuve par le texte[511].

[505] Organisations : Bär & Karrer, SWICO.

[506] Dans le sens où le traitement ne présente pas un risque élevé pour la personne concernées si ces conditions ne sont pas remplies. Organisations : Bär & Karrer, SWICO.

[507] Organisations : ASB, IGEM, suva, VUD.

[508] Organisations : ASPS, Association de commerce, CURAVIVA, EXPERTsuisse, FMH, IGEM, INSOS, IS, senesuisse, Spitex suisse, SSMD, suva, UPSV, usam, VUD.

[509] Organisations : ASPS, CURAVIVA, INSOS, IS, senesuisse, Spitex suisse.

[510] Organisations : ASB, FSA, IGEM, santésuisse, VUD.

[511] Organisations : ASSL, auto suisse, economiesuisse, Swiss Insights, UPSA, usam.

3.2.27 Art. 27 P-OLPD : Désignation

Il est reproché à cet article de manquer de proportionnalité et d'être impossible à mettre en œuvre en pratique, dans la mesure où chaque organe fédéral doit nommer son propre conseiller à la protection des données[512]. De plus, l'UTP est d'avis que l'obligation de désigner un conseiller à la protection des données est dépourvue de base légale. Le canton de Schwyz fait remarquer que la loi sur la protection des données Schengen exige l'intervention de conseillers à la protection des données uniquement dans les domaines de la police, de la poursuite pénale et de l'exécution des peines. D'autres participants soulignent que l'actuel art. 23 OLPD prévoit la désignation de conseillers à la protection des données pour la Chancellerie fédérale et pour chacun des sept départements fédéraux. Néanmoins, les offices fédéraux sont bien plus nombreux, raison pour laquelle il serait préférable de conserver la formulation actuelle[513].

Au contraire, le PS est favorable au fait que chaque organe fédéral soit tenu de désigner son propre conseiller à la protection des données. Il motive cet avis d'une part par le fait que tous les organes fédéraux ont une envergure suffisante en termes de nombre de collaborateurs et de quantité de données à traiter, de sorte qu'il se justifie qu'ils disposent de leurs propres conseillers à la protection des données, et d'autre part, par le fait que les conseillers internes disposent d'une meilleure connaissance de la culture institutionnelle et des collaborateurs de l'organe concerné, et sont par conséquent mieux à même d'assumer leurs tâches de manière efficace. L'UTP considère également que, pour remplir correctement leurs tâches, les conseillers à la protection des données doivent être familiers des processus de l'institution concernée, et qu'il serait partant peu judicieux de désigner des conseillers à la protection des données personnelles pour plusieurs organes fédéraux.

L'ASA refuse entièrement la désignation de conseillers à la protection des données personnelles pour les organes fédéraux. Elle est d'avis que cette désignation devrait également avoir lieu sur une base volontaire et qu'une mesure incitative devrait être créée en ce sens. L'ASIP souhaite l'instauration d'une exception à l'obligation de désigner des conseillers à la protection des données personnelles pour les institutions de prévoyance enregistrées au sens de l'ordonnance des 11 et 22 juin 2011 sur la surveillance dans la prévoyance professionnelle[514] **.**

Le canton de Fribourg déplore que la disposition omette de préciser de quelle manière l'indépendance des conseillers à la protection des données doit être garantie, ainsi que les sanctions prévues en cas de non-respect de cette exigence d'indépendance. De plus, il est d'avis que la relation entre les conseillers à la protection des données personnelles et les préposés à la sécurité de l'information doit être précisée. Ces tâches pourraient éventuellement être confiées à une seule personne.

3.2.28 Art. 28 P-OLPD : Exigences et tâches

Titre

HÄRTING regrette le titre de cette disposition, et estime qu'il doit être précisé afin de clarifier que la norme s'applique exclusivement aux organes fédéraux.

[512] Canton : SZ; organisations : CP, FER, UTP.

[513] Organisations : CP, FER.

[514] OPP 1 ; RS **831.435.1**.

Al. 2

Let. a

SwissICT souhaite qu'on biffe la let. a de l'al. 2, car il est d'avis que cette obligation générale de contrôle va trop loin. Selon lui, les conseillers à la protection des données peuvent agir uniquement en tant que points de contact[515]. Classtime préconise l'introduction à l'al. 2, let. a de « catégories de sensibilité », au motif que le contrôle du traitement des données personnelles devrait s'inscrire dans le contexte des cas d'application, de l'utilité du traitement et de la sensibilité des données.

Les cantons et privatim regrettent le fait que seule la tâche de formation et de conseil soit mentionnée ici, et non la tâche fixée à l'art. 10, al. 2 LPD de concourir à l'application des prescriptions relatives à la protection des données. Ils souhaitent que l'article soit complété en ce sens[516].

3.2.29 Art. 29 P-OLPD : Devoirs de l'organe fédéral

Al. 1

Le canton de Schwyz relève que les conseillers à la protection des données personnelles ne sont pas délégués par l'organe de surveillance, mais des conseillers internes, des interlocuteurs de l'organe de surveillance et des points de contact pour l'organe public responsable. Partant, il s'oppose à ce que des droits d'accès étendus soient ancrés dans la loi. Dans le même ordre d'idées, swissICT fait remarquer que l'accès doit impérativement avoir lieu en relation avec les tâches attribuées aux conseillers à la protection des données personnelles, raison pour laquelle la formulation prévue va trop loin.

Al. 2

Peu d'intervenants souhaitent que la disposition soit précisée par l'exigence de publication d'une adresse e-mail de fonction, ce dans l'intérêt de la protection de la personnalité des conseillers à la protection des données personnelles[517].

3.2.30 Art. 30 P-OLPD : Interlocuteur du PFPDT

Santésuisse relève qu'en raison de la réduction drastique des compétences des conseillers internes à la protection des données, il deviendra difficile pour eux d'interagir avec le PFPDT. Elle estime que l'indépendance dont ils jouissent actuellement sera restreinte par le volet « conseil » de leur activité.

3.2.31 Art. 31 P-OLPD : Information du conseiller à la protection des données

Plusieurs participants font remarquer que cette disposition ne repose pas sur une base légale suffisante. De tels devoirs d'information et d'annonce devraient être réglés dans la loi[518]. SwissICT relève que le traitement automatisé des données personnelles est courant, et que le législateur ne peut avoir souhaité soumettre les projets de traitement automatisé des données à une obligation d'autorisation aussi générale. En effet, l'art. 35, al. 1 nLPD prévoit

[515] À ce sujet, voir les commentaires sous l'art. 25 P-OLPD.

[516] Cantons : AG, TG, SH, VD; organisation : privatim.

[517] Organisations : BNS, dans le même sens également ASA, Walderwyss.

[518] Organisations : ASA, Curafutura.

l'obligation d'autorisation uniquement pour ce qui a trait au traitement automatisé de données sensibles. Partant, il convient de compléter le projet d'ordonnance en ce sens[519].

L'ASA refuse l'obligation imposée aux organes fédéraux d'informer leurs conseillers à la protection des données en cas de projets de traitement automatisé de données personnelles. Cette obligation n'apporte aucune valeur ajoutée aux personnes concernées et engendrerait une charge administrative inutile. C'est pourquoi cette disposition doit selon elle être supprimée.

En faisant la comparaison avec l'OLPD en vigueur, l'UPSV regrette que la notion d'« information immédiate » ait été remplacée par celle d'« information en temps utile ». Du fait que la notion de « temps utile » nécessite un travail d'interprétation, elle mettrait en danger la sécurité du droit et son application uniforme. On court ainsi le risque de légitimer d'éventuels retards dans la transmission d'informations. La notion initiale d'« immédiateté » devrait ainsi être conservée.

En revanche, d'autres participants souhaitent que le terme « à temps » qui figure en fin de phrase soit également remplacé par « en temps utile ». Selon eux, la signification du terme « à temps » n'est pas claire. Par ailleurs, ils estiment qu'il est suffisant que les exigences de la protection des données soient prises en compte en temps utile dans le projet[520]. La BNS souhaite qu'« à temps » soit remplacé par « de manière appropriée » ou qu'il soit supprimé, ce qui lui semble également possible. Curafutura estime que l'expression « après l'achèvement du projet » n'est pas claire.

Les CFF sont d'avis que la disposition fixe des exigences de nature purement interne et qu'elle porte ainsi une atteinte disproportionnée à la liberté d'organisation des entreprises de transport. Les « entreprises » responsables devraient être libres de définir de quelle manière elles entendent mettre en œuvre leurs propres méthodes et processus. En effet, toutes les « entreprises » n'utilisent pas la méthode HERMES pour gérer leurs projets. Selon SwissICT, cette disposition ne saurait s'appliquer en l'état aux organes fédéraux externes comme les caisses de pension, car celles-ci sont parfois soumises à des obligations de confidentialité fondées sur des lois spéciales.

3.2.32 Art. 32 P-OLPD : Annonce au PFPDT

Certains participants préconisent la suppression de cette norme[521]. Celle-ci ne repose sur aucune base légale[522]. Dans la partie du message consacrée à l'art. 12, al. 4, nLPD, il est précisé qu'il ne devrait pas y avoir de changement par rapport au droit en vigueur. Il n'existe toutefois pas encore d'obligation d'annoncer les banques de données qu'il est prévu de créer au PFPDT[523].

[519] Organisations : HÄRTING.

[520] Organisations : DFS, IGEM, suva, VUD.

[521] Organisations : BNS, Curafutura, IGEM, suva, SWICO, swissICT, VUD.

[522] Organisations : ASA, BNS, Curafutura, DFS, IGEM, santésuisse, suva, SWICO, swissICT, VUD, Walderwyss.

[523] Organisations : BNS, IGEM, suva, VUD.

Certains critiquent également le fait que les activités déjà prévues de traitement automatisé doivent être annoncées[524]. Le texte prévoit que l'annonce doit avoir lieu au moment de l'approbation du projet ou de la décision de le développer[525]. C'est pourquoi certains participants remettent fortement en cause la proportionnalité de l'art. 32, al. 1[526]. Selon plusieurs avis, cette disposition augmente de manière considérable le travail (administratif) nécessaire à la documentation[527]. En effet, les décisions concrètes sont la plupart du temps prises en cours de projet seulement, raison pour laquelle les informations exigées ne sont tout simplement pas encore disponibles ou ne sont pas encore suffisamment détaillées au moment où elles doivent être fournies[528]. Les CFF observent également que la disposition ne pourrait concrètement s'appliquer à ses propres projets, qui ne sont plus planifiés selon le « modèle en cascade » classique, mais de manière agile. Les notions utilisées dans la disposition sont également considérées comme obsolètes. D'autres participants relèvent en outre que le fait de savoir à partir de quand un traitement est « prévu » n'est pas clair[529].

Un autre motif pour lequel la charge de travail supplémentaire engendrée par cette annonce précoce n'est pas justifiée est le fait que, conformément au rapport explicatif, cette annonce n'a pas pour but la protection de la personnalité, mais la planification des ressources du PFPDT[530]. Walderwyss considère que le PFPDT ne pourrait de toute façon rien faire de ces informations, car il ne dispose pas des ressources nécessaires pour assurer le suivi.

Un autre problème soulevé est que l'obligation d'annonce porte sur chaque projet de traitement automatisé et non seulement sur ceux qui présentent un risque potentiellement élevé[531]. Les CFF sont d'avis que l'obligation d'annonce au PFPDT de chaque traitement non manuel augmenterait de manière disproportionnée la charge de travail et ne serait pas propre à atteindre l'objectif poursuivi. En outre, cela serait contraire à l'approche fondée sur le risque suivie par la nLPD. D'autres participants soulignent également que, si l'art. 47 P-OLPD constitue effectivement une disposition transitoire pour les activités de traitement automatisé, cette disposition n'a toutefois pas pour effet de faciliter la situation, car un registre doit être établi pour les traitements déjà en phase de production et doit être annoncé au PFPDT[532].

Les CFF font remarquer que selon le droit en vigueur, il n'existe aucune obligation pour les entreprises de transport d'annoncer les fichiers au PFPDT. Les entreprises de transport qui nomment des conseillers à la protection des données devraient continuer à être exemptées de l'obligation d'annonce au PFPDT.

3.2.33 Art. 33 P-OLPD : Caractère indispensable de la phase d'essai

Le canton de Vaud observe que l'on devrait prévoir une obligation de consulter les autorités cantonales lorsque les projets les impliquent également.

SwissICT indique qu'il convient de prévoir une obligation d'autorisation uniquement lorsque le traitement a un impact important sur des données sensibles. Il préconise en outre de biffer la let. c, car il s'agit uniquement d'un cas de figure possible qui doit être examiné. Dans le

[524] Organisations : BNS, Curafutura, DFS, IGEM, suva, SWICO, swissICT, VUD.

[525] Organisations : BNS, CFF, IGEM, santésuisse, suva, SWICO, swissICT, VUD, Walderwyss.

[526] Organisations : BNS, Walderwyss.

[527] Organisations : BNS, Curafutura, DFS, IGEM, suva, SWICO, swissICT, VUD.

[528] Organisations : BNS, CFF, IGEM, santésuisse, suva, SWICO, swissICT, VUD, Walderwyss.

[529] Organisations : BNS, Walderwyss.

[530] Organisations : ASA, CFF, Curafutura, DFS, IGEM, santésuisse, suva, VUD.

[531] Organisations : BNS, Santésuisse, SWICO.

[532] Organisations : IGEM, santésuisse, suva, VUD.

même ordre d'idées, HÄRTING souhaite que la phase d'essai, en tant qu'essai pilote, dépende de l'existence d'un risque élevé pour la personne concernée.

3.2.34 Art. 34 P-OLPD : Autorisation

SwissICT relève que la disposition ne mentionne ni la sanction encourue en cas de non-respect de la nLPD, ni les conditions de retrait de l'autorisation. En particulier, il serait judicieux d'y indiquer également la procédure prévue ainsi que les délais.

Al. 2

Santésuisse souhaiterait que, dans un but de sécurité de la planification, l'on définisse le délai le PFPDT pendra position.

De plus, SwissICT trouverait judicieux que la let. d utilise l'expression de « mesures techniques et organisationnelles » en lieu et place des « mesures de sécurité et de protection des données ». Il propose en outre la suppression de la let. e, car un projet d'ordonnance n'est pas nécessaire dans chaque situation.

Al. 5

S'agissant de l'al. 5, SwissICT trouve qu'il n'est pas clair de savoir si une proposition doit être adressée au Conseil fédéral dans tous les cas.

3.2.35 Art. 35 P-OLPD : Rapport d'évaluation

Selon SwissICT, il sied de préciser que le rapport doit être utilisé pour les étapes ultérieures.

3.2.36 Art. 36 P-OLPD : Traitements à des fins ne se rapportant pas à des personnes

Des participants font remarquer que la disposition est superflue, car cette précision figurant à l'art. 36 P-OLPD ressort déjà de l'art. 39 nLPD[533]. L'ASA ajoute que, pour ce motif, cette disposition de l'ordonnance ne fait qu'engendrer de la confusion et créé une insécurité juridique.

SwissICT relève que l'art. 39 nLPD s'applique de toute façon uniquement au traitement à des fins ne se rapportant pas à des personnes effectué par des organes fédéraux dans le cadre de la recherche, de la planification ou de la statistique. Ces organes fédéraux ne devraient pas avoir à distinguer si un traitement destiné à la recherche, à la planification ou à la statistique, présente éventuellement aussi une composante se rapportant à des personnes.

3.2.37 Art. 39 P-OLPD : Communication des directives et des décisions

L'UPSV note qu'il serait judicieux d'indiquer directement dans l'ordonnance le moment auquel le PFPDT doit être impliqué dans les projets législatifs concernant la protection des données personnelles et l'accès aux documents officiels. Cela permettrait de créer de la sécurité juridique et d'éviter toute interprétation.

Le DFS se demande pourquoi l'administration fédérale doit communiquer ses directives au PFPDT sous une forme anonymisée. Les directives en matière de protection des données sont des conditions-cadres adressées à plusieurs destinataires et devraient ainsi en règle générale être soumises au principe de transparence.

[533] Cantons : AG, AI, GR, NW, SH, SZ, VD, ZH ; organisations : Préposé à la protection des données de SZ, OW et NW, privatim, ASA, swissICT.

3.2.38 Art. 41 P-OLPD : Autocontrôle

Santésuisse suggère que le PFPDT soit également soumis à l'obligation de tenir un registre des activités de traitement. Il n'existe aucune raison pour qu'il soit libéré de cette obligation[534].

Classtime est d'avis que l'autocontrôle ne devrait pas seulement être imposé au PFPDT, mais aussi aux prestataires privés et aux autorités fédérales dans le cadre des principes d'autorégulation.

3.2.39 Art. 42 P-OLPD : Collaboration avec le Centre national pour la cybersécurité (NCSC)

HDC reproche à la disposition d'utiliser à son al. 1 l'expression de « personne responsable de l'annonce », qui ressemble à la « personne tenue d'annoncer » figurant à l'art. 24, al. 6, nLPD. Il serait préférable d'utiliser la notion de personne responsable du traitement[535].

3.2.40 Art. 43 P-OLPD : Registre des activités de traitement des organes fédéraux

Les CFF se réfèrent à l'art. 27 P-OLPD et expriment à nouveau le souhait que les entreprises de transport qui désignent un conseiller à la protection des données soient dispensées, comme c'est déjà le cas actuellement, de l'obligation de déclarer leur registre d'activités de traitement au PFPDT selon l'art. 12, al. 4, nLPD. De plus, le registre de l'ensemble des activités de traitement est réputé secret d'affaires et ne saurait être rendu accessible sans limitation au public.

Curafutura fait remarquer qu'en cas de suppression de l'art. 32 P-OLPD, l'art. 43 P-OLPD devrait être adapté en conséquence[536].

3.2.41 Art. 44 P-OLPD : Code de conduite

La FER trouve regrettable que la prise de position du PFPDT ne soit pas une décision au sens formel (décision pouvant faire l'objet d'un recours). D'autre part, dans la mesure où le PFPDT facture un émolument pour rendre une prise de position, elle souhaite qu'un délai soit prévu pour rendre la prise de position, et que ce délai ne soit pas trop long. Elle considère un délai de maximum 30 jours comme opportun.

3.2.42 Art. 45 P-OLPD : Émolument

En général

D'une manière générale, plusieurs participants reprochent à la disposition d'inciter les organisations à enfreindre le droit de la protection des données en raison du coût élevé fixé pour l'assistance du PFPDT[537]. C'est pourquoi il convient de remanier entièrement la règle applicable à l'émolument et de la modifier pour l'adapter dans une mesure raisonnable[538]. Santésuisse est favorable au fait de ne prélever aucun émolument. Certains participants soulignent que le seuil d'accès au PFPDT doit être maintenu à un bas niveau, tout particulièrement eu égard à la vérification du caractère adéquat des codes de conduite (art. 59, al. 1,

[534] Organisations : HÄRTING.

[535] Organisations : Swissprivacy.law.

[536] Organisations : ASA.

[537] Organisations : ASP, ASPS, Creditreform, CURAVIVA, EPS, FSEP, INSOS, IS, santésuisse, senesuisse, Spitex suisse, usam, vsi.

[538] Organisations : ASP, ASPS, Creditreform, CURAVIVA, EPS, FSEP, INSOS, IS, senesuisse, Spitex suisse, usam, vsi.

let. a, nLPD) ou à l'approbation des clauses type de protection des données (art. 59, al. 1, let. b, nLPD)[539].

Al. 1

Certains participants soulignent que les émoluments ne devraient pas être calculés en fonction du temps consacré, car les entreprises n'ont d'influence ni sur la complexité de la problématique, ni sur l'efficacité du PFPDT[540]. Il est proposé de fixer un plafond pour les émoluments[541].

Al. 2

Certains participants considèrent que le tarif horaire qui varie entre 150 et 350 CHF est beaucoup trop élevé, voire dissuasif[542]. Il est souligné qu'il existe une discrépance entre les émoluments du PFPDT et la participation aux frais des individus en cas de demandes de renseignement[543]. Les activités du PFPDT sont pourtant dans l'intérêt de la société et du public. Il n'existe aucun motif raisonnable pour que les organisations qui ont besoin de ses services pour se conformer au droit de la protection des données, doivent assumer des frais aussi élevés. Cela va à l'encontre du principe même de service public[544]. Spitex fait remarquer qu'en particulier pour le domaine des entreprises actives dans le domaine de la santé, il conviendrait de prévoir une exception avec des tarifs horaires raisonnables[545].

La SPA souhaite que le PFPDT informe à l'avance sur les émoluments escomptés.

3.2.43 Art. 47 P-OLPD : Disposition transitoire concernant l'annonce au PFPDT des activités prévues de traitement automatisé

Certains participants font remarquer qu'en cas de suppression de l'art. 32 P-OLPD, l'art. 47 P-OLPD devrait également être biffé[546].

3.2.44 Art. 48 P-OLPD : Entrée en vigueur

Certains participants relèvent que la nouvelle LPD ne contient pas de délais transitoires, ou seulement des délais ponctuels et lacunaires[547]. C'est pourquoi le nouveau droit devrait déjà être entièrement mis en œuvre lors de son entrée en vigueur[548]. Toutefois, la version définitive de l'ordonnance devrait être disponible et rendue accessible au public au plus tôt fin 2021. Actuellement, le DFJP prévoit la mise en vigueur du nouveau droit au cours du deuxième semestre 2022[549].

[539] Organisations : ASPS, CURAVIVA, INSOS, IS, senesuisse, Spitex suisse.

[540] Organisations : ASP, ASPS, Creditreform, CURAVIVA, EPS, FSEP, GastroSuisse, INSOS, IS, senesuisse, Spitex suisse, usam, vsi.

[541] Organisations : ASP, CP, Creditreform, EPS, FER, FSEP, vsi.

[542] Organisations : ASP, ASPS, Creditreform, CURAVIVA, EPS, FSEP, INSOS, IS, senesuisse, Spitex suisse, usam, vsi.

[543] Organisations : ASP, Creditreform, EPS, FSEP, usam, vsi.

[544] Organisations : ASP, Creditreform, EPS, FSEP, GastroSuisse, vsi.

[545] Organisations : ASPS, CURAVIVA, INSOS, IS, senesuisse, Spitex suisse.

[546] Organisations : ASA, Curafutura.

[547] Organisations : ASA, ASB, Economiesuisse, santésuisse.

[548] Organisations : ASA, Santésuisse.

[549] Organisation: Santésuisse.

Afin d'assurer une mise en œuvre correcte du nouveau droit, il convient toutefois d'attendre la version définitive de l'ordonnance[550]. Ce n'est qu'ensuite qu'il sera possible de débuter l'adaptation des processus, respectivement la mise en œuvre et le renforcement des solutions basées sur les technologies de l'information. Avant l'activation de ces systèmes, des tests devront également encore être effectués. De plus, les collaborateurs devront être formés selon leurs fonctions respectives[551].

Il résulte de ce qui précède que le délai de mise en œuvre de 6 mois est extraordinairement court. Santésuisse est d'avis que, pour la plupart des entreprises, cela n'est pas réalisable. En effet, comme le relève un petit nombre de participants, le nouveau paquet législatif est extrêmement complexe et exige de nombreuses adaptations[552]. Il conviendrait d'avoir nettement plus de temps pour adopter une approche aussi globale que possible dans la mise en œuvre[553]. L'ASB et economiesuisse sont d'avis qu'une période de deux ans environ serait nécessaire pour les activités mentionnées ci-dessus. L'ASA évalue cette période à une année environ.

Dans l'UE, deux ans avaient été prévus pour la mise en application de l'ensemble du RGPD. Le Parlement suisse a quant à lui pris une autre décision de principe pour la nLPD. Néanmoins, les dispositions transitoires prévues lors du processus parlementaire s'avèrent souvent trop courtes. À cela s'ajoute que les dispositions transitoires doivent être fixées uniquement sur la base de critères objectifs. C'est pourquoi il est devenu courant de fixer si nécessaire des dispositions transitoires complémentaires au niveau de l'ordonnance. Selon certains participants, il va de soi qu'un report de l'entrée en vigueur de l'intégralité du paquet législatif au 1er juillet 2023 serait également envisageable[554].

Partant, certains participants proposent de reporter la mise en vigueur au 1er janvier 2023 au plus tôt[555]. Une autre proposition consiste à compléter ce régime transitoire lacunaire au niveau de l'ordonnance en y ajoutant d'autres dispositions transitoires. En particulier, des délais transitoires adaptés devraient être prévus pour toutes les nouvelles obligations qui engendrent un travail considérable. C'est le cas à tout le moins pour l'obligation d'assurer une sécurité adéquate des données (art. 8 nLPD, en relation avec l'art. 19 P-OLPD), pour l'obligation de tenir un registre des activités de traitement (art. 12 nLPD), ainsi que pour l'obligation d'annoncer dans les meilleurs délais les cas de violation de la sécurité des données (art. 24 nLPD, en relation avec l'art. 19 P-OLPD). Pour ces obligations, et malgré le fait qu'elles existent déjà actuellement, un délai transitoire jusqu'au 1er juillet 2023 au moins est préconisé[556].

3.3 Annexe 2

3.3.1 Ordonnance VOSTRA

Le canton de Soleure fait remarquer que l'art. 18 de l'ordonnance VOSTRA du 29 septembre 2006[557] prévoit que les données du casier judiciaire au sens de l'art. 366, al. 2 à 4, CP, ne peuvent pas être enregistrées ou conservées de manière isolée dans une nouvelle banque

[550] Organisations : ASA, ASB, Economiesuisse, santésuisse.

[551] Organisations : ASA, ASB, Economiesuisse.

[552] Organisations : AFBS, ASA.

[553] Organisations : AFBS, ASB, economiesuisse.

[554] Organisations : ASB, Economiesuisse.

[555] Organisations : AFBS, santésuisse.

[556] Organisations : ASB, Economiesuisse.

[557] RS **331.**

de données, à moins que cela soit nécessaire pour motiver une décision rendue, une disposition édictée ou pour justifier une étape de procédure engagée. Cependant, avec l'entrée en vigueur de la nouvelle loi sur le casier judiciaire prévue en 2023, les services de police cantonaux auront accès au casier judiciaire. Il contient notamment des informations relatives aux renvois et aux interdictions d'accès au sens du CC et de la législation cantonale. Ces données seront également à disposition des membres de la police qui interviennent sur place dans une optique de limitation des risques et de prévention des infractions pénales. Le canton de Soleure estime qu'il devrait en être de même pour les interdictions prévues aux art. 67 ss. CP. C'est pourquoi la disposition devrait être complétée en ajoutant que les données sont également nécessaires pour « mettre œuvre » une décision qui a été rendue *(« zur Durchsetzung eines getroffenen Entscheids »).*

3.3.2 Annexe relative à l'ordonnance sur les relevés statistiques

Le canton de Vaud relève, au sujet de cette annexe, que selon le ch. 72, titre, 2e ligne, 2e colonne et 9e ligne, 2e colonne, il est possible d'utiliser certaines informations dans certains buts administratifs avec l'accord des intéressés. Cela figure déjà à l'annexe de l'ordonnance actuelle sur les relevés statistiques, or cette possibilité est une dérogation importante aux principes régissant les traitements de données statistiques. Il propose de compléter par des exemples de ce que l'on entend par « dans certains buts administratifs ».

3.3.3 Ordonnance VIS

Au sujet de l'art. 31, al. 1 de l'ordonnance VIS du 18 décembre 2013[558] la FER fait remarquer qu'il manque un pronom dans la version française. Il faudrait rajouter « elle » pour obtenir « Si une personne [...], **elle** présente une demande écrite au SEM [...] ».

3.3.4 Ordonnance sur le service de l'emploi

En ce qui concerne l'ordonnance du 16 janvier 1991 sur les services de l'emploi[559], la FER relève que l'art. 19, al. 2, let. c, nLPD prévoit que lors de la collecte, le responsable du traitement communique à la personne concernée les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la loi et pour que la transparence des traitements soit garantie. Il communique au moins, le cas échéant, les destinataires ou les *catégories de destinataires* auxquels les données personnelles sont transmises. La FER considère que l'art. 58, al. 1, let. d, OSE devrait reprendre le libellé de la nLPD. Il devrait être écrit « Le cas échéant, des *catégories de* destinataires auxquelles des données sont transmises » (et non pas « le cas échéant, des destinataires auxquelles des données sont transmises »).

Le FER est d'avis que, dès lors que l'art. 19, al. 2, let. a, nLPD mentionne « l'identité et les coordonnées du responsable du traitement », l'art. 58 al. 1, let. a, OSE doit être supprimé faute de base légale. En effet, dite disposition de l'OSE propose des termes différents de la nLPD, notamment « l'identité et les coordonnées du responsable du système d'information ».

Enfin, elle ajoute que les remarques indiquées à l'art. 58 OSE doivent également valoir pour l'art. 126 OACI[560].

[558] RS **142.512**.

[559] OSE; RS **823.111**.

[560] Ordonnance du 31 août 1983 sur l'assurance-chômage ; RS **837.02**.

4 Consultation des documents

Conformément à l'article 9 de la loi fédérale du 18 mars 2005 sur la procédure de consultation[561], sont accessibles au public : le dossier soumis à consultation et, après expiration du délai de consultation, les avis exprimés par les participants à la consultation, ainsi que, après la prise de connaissance par le Conseil fédéral de ce rapport, le rapport rendant compte des résultats de la consultation. Ces documents sont publiés sous forme électronique sur le site Internet de la Chancellerie fédérale[562].

[561] RS **172.061**.

[562] www.fedlex.admin.ch > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2021 > EJPD.

5 Glossaire

AIPD / DSFA	Analyses d'impact de protection des données / Datenschutz-Folgen-abschätzung
AP-OLPD / VE-VDSG	Avant-projet de l'Ordonnance relative à la loi fédérale sur la protection des données / Vorentwurf der Verordnung zum Bundesgesetz über den Datenschutz
Art.	Article / Artikel
ATF / BGE	Arrêt du Tribunal fédéral / Bundesgerichtsentscheid
BCR	Binding Corporate Rules
CAID / CIA	Confidentialité, Authenticité, Intégrité, Disponibilité / Vertraulichkeit, Integrität, Verfügbarkeit
ch. / ziff.	Chiffre / Ziffer
CHF	Franc suisse / Schweizer Franken
E-ID	Identité électronique / Elektronische Identität
IA / KI	Intelligence artificielle / Künstliche Intelligenz
ICT	Information and Communication Technology
ISO / OIN	Organisation internationale de normalisation / Internationale Organisation für Normung
IT	Information Technology
Let. / Lit.	Lettre / Litera
nLPD / nDSG	Loi fédérale du 25 septembre 2020 sur la protection des données / Bundesgesetz vom 25. September 2020 über den Datenschutz
OLPD / VDSG	Ordonnance fédérale du 14 juin 1993 relative à la loi fédérale sur la protection des données / Verordnung zum Bundesgesetz über den Datenschutz (Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz
p. ex. / z.B.	par exemple / zum Beispiel
para. / Abs.	paragraphe / Absatz
PFPDT / EDÖB	Le préposé fédéral à la protection des données et à la transparence / Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte
PME / KMU	Petite ou moyenne entreprise / Kleine und mittlere Unternehmen
P-OLPD / E-VDSG	Projet d'ordonnance relative à la loi fédérale sur la protection des données / Entwurf zur Verordnung zum Bundesgesetz über den Datenschutz
resp. / bzw.	respectivement / Beziehungsweise
RGPD / DSGVO	Règlement européen sur la protection des données / Datenschutz-Grundverordnung der Europäischen Union
SA / AG	Société anonyme / Aktiengesellschaft

Sàrl / GmbH	Société à responsabilité limitée / Gesellschaft mit beschränkter Haftung
TAF / BVGer	Tribunal administratif fédéral / Bundesverwaltungsgericht
UE / EU	Union européenne / Europäische Union

6 Annexe

Liste des organismes ayant répondu
Verzeichnis der Eingaben
Elenco dei partecipanti

Cantons / Kantone / Cantoni

AG		Argovie / Aargau / Argovia
AI		Appenzell Rh.-Int. / Appenzell Innerrhoden / Appenzello Interno
AR		Appenzell Rh.-Ext. / Appenzell Ausserrhoden / Appenzello Esterno
BE		Berne / Bern / Berna
BL		Bâle-Campagne / Basel-Landschaft / Basilea-Campagna
BS		Bâle-Ville / Basel-Stadt / Basilea-Città
FR		Fribourg / Freiburg / Friburgo
GE		Genève / Genf / Ginevra
GL		Glaris / Glarus / Glarona
GR		Grisons / Graubünden / Grigioni
LU		Lucerne / Luzern / Lucerna
NE		Neuchâtel / Neuenburg
NW		Nidwald / Nidwalden / Nidvaldo
OW		Obwald / Obwalden / Obvaldo
SG		Saint-Gall / St. Gallen / San Gallo
SH		Schaffhouse / Schaffhausen / Sciaffusa
SO		Soleure / Solothurn / Soletta
SZ		Schwyz / Svitto
TG		Thurgovie / Thurgau / Turgovia
TI		Tessin / Ticino
UR		Uri
VD		Vaud / Waadt
VS		Valais / Wallis / Vallese
ZH		Zurich / Zürich / Zurigo

Partis politiques / Parteien / Partiti politici

le Centre / die Mitte	Le Centre Die Mitte Alleanza del Centro
PLR / FDP	PLR. Les Libéraux-Radicaux FDP. Die Liberalen PLR. I Liberali Radicali PLD. Ils Liberals

PPS	Parti pirate suisse PPS Piratenpartei Schweiz PPS Partito pirata Svizzeri PPS
PS / SP	Parti socialiste suisse PS Sozialdemokratische Partei der Schweiz SP Partito socialista svizzero PS
PVS / GPS	Parti les VERT-E-S suisse PVS Grüne Partei der Schweiz GPS Partito dei Verdi Svizzeri PVS
UDC / SVP	Union démocratique du centre UDC Schweizerische Volkspartei SVP Unione democratica di centro UDC

Organisations intéressées et particuliers / Interessierte Organisationen und Privatpersonen / Organizzationi interessate e privati

ADIDE	Association pour le dictionnaire des droits de l'enfant
AFBS	Association of Foreign Banks in Switzerland Verband der Auslandbanken in der Schweiz Association des banques étrangères en Suisse Associazione delle banche estere in Svizzera
ASA / SVV	Association Suisse d'Assurances Schweizerischer Versicherungsverband Associazione Svizzera d'Assicurazioni Swiss Insurance Association
ASB / SBVg	Association suisse des banquiers Schweizerische Bankiervereinigung Associazione Svizzera die Banchieri Swiss Bankers Association
ASDPO	Association Suisse des Délégués à la Protection des Données
ASIP	Association suisse des Institutions de prévoyance Schweizerischer Pensionskassenverband Associazione svizzera delle Istituzioni di previdenza
ASP / RVS	Association Suisse du Pneu Reifen-Verband der Schweiz Associazione svizzera del pneumatico
ASPS	Association Spitex privée Suisse
ASSL / SLV	Association Suisse des Sociétés de Leasing Schweizerischer Leasingverband
Association de commerce / HANDELSVERBAND.swiss	Association de commerce Handelsverband

asut	Association Suisse des Télécommunications Schweizerischer Verband der Telekommunikation Swiss Telecommunications Association
ATPrD / ÖDSB	Autorité cantonale de la transparence et de la protection des données (Fribourg) Kantonale Behörde für Öffentlichkeit und Datenschutz (Fribourg)
auto suisse / auto schweiz	Vereinigung Schweizer Automobil-Importeure
Bär & Karrer	Bär & Karrer AG
Beat Lehmann	Lic. Iur. Führsprecher
Bibliosuisse	Bibliosuisse
BNS / SNB	Banque Nationale Suisse Schweizerische Nationalbank Banca Nazionale Svizzera Banca Naziunala Svizera Swiss National Bank
CFC / EKK	Commission fédérale de la consommation CFC Eidgenössische Kommission für Konsumentenfragen
CFF / SBB	CFF SBB FFS
Classtime	Classtime AG
Coop	Coop Genossenschaft
CP	Centre Patronal
Creditreform	Creditreform Egeli Vogel Bern AG
curafutura	Les assureurs-maladie innovants Die innovativen Krankenversicherer Gli assicuratori-malattia innovativi
CURAVIVA	CURAVIVA suisse CURAVIVA Schweiz
CYBER SAFE	Association Suisse pour le Label de Cybersécurité
Datenschutzguide.ch	Datenschutzguide.ch GmbH c/o gbf Rechtsanwälte AG
DFS	Datenschutz Forum Schweiz
DigiGes	Digitale Gesellschaft
digitalswitzerland	digitalswitzerland Initiative
economiesuisse	Fédération des entreprises suisses Verband der Schweizer Unternehmen Federazione delle imprese svizzere Swiss Business Federation

EPS / PBS	Education Privée Suisse Private Bildung Schweiz Swiss Private Education Educazione Privata Svizzera
ETH-Bibliothek	Bibliothek der Eidgenössischen Technischen Hochschule Zürich
EXPERTsuisse	EXPERT SUISSE Wirtschaftsprüfung/Steuern/Treuhand
FER	Fédération des Entreprises Romandes
FMH	Fédération des médecins suisses Verbindung der Schweizer Ärztinnen und Ärzte Federazione dei medici svizzeri Foederatio Medicorum Helveticorum
Forum PME / KMU-Forum	Forum PME KMU-Forum Forum PMI
FRC	Fédération romande des consommateurs
FSA / SAV	Fédération Suisse des Avocats Schweizerischer Anwaltsverband Federazione Svizzera degli Avvocati Swiss Bar Association
FSEP / VSP	Fédération suisse des écoles privées Verband Schweizerischer Pritvatschulen Federazione svizzera delle scuole private
GastroSuisse	Pour l'Hôtellerie et la Restauration Für Hotellerie und Restauration Per l'Albergheria e la Ristorazione
H+	Les hôpitaux de Suisse Die Spitäler der Schweiz Gli ospedali Svizzeri
HÄRTING / HÄRTING Rechtsanwälte	HÄRTING Rechtsanwälte AG
HDC	HDC law firm étude d'avocats
HKBB	Handelskammer beider Basel
HotellerieSuisse	Schweizerischer Hotellerie Verband
IGEM	Interessengemeinschaft elektronische Medien
INSOS	INSOS Schweiz
IS / AIS	Insertion Suisse Arbeitsintegration Schweiz Inserimento Svizzera
la Poste / die Post	La Poste Suisse SA Die Schweizerische Post AG

les banques domestiques / die Inlandbanken	Les banques domestiques Verband Schweizer Regionalbanken Verband Schweizer Kantonalbanken Migros Bank AG Raiffeisen Schweiz Genossenschaft
Migros	Migros Genossenschaft
pharmaSuisse	Schweizerischer Apothekerverband
Préposé à la protection des données de SZ, OW et NW / Datenschutzbeauftragter SZ/OW/NW	Préposé à la protection des données des cantons de Schwyz, Obwald et Nidwald Datenschutzbeauftragter Schwyz Obwalden Nidwalden
Préposé cantonal à la protection des données et à la transparence NE/JU	Préposé cantonal à la protection des données et à la transparence des cantons de Neuchâtel et Jura
Privacy Icons	Privacy Icons c/o Wenger & Vieli AG
privatim	Conférence des préposé(e)s suisse à la protection des données Konferenz der schweizerischen Datenschutzbeauftragten Conferenza degli incaricati svizzeri per la protezione die dati
proFonds	Dachverband gemeinütziger Stiftungen der Schweiz
Raiffeisen	Banque Raiffeisen Raiffeisenbank
rega	Garde aérienne suisse de sauvetage Schweizerische Rettungsflugwacht Guardia aerea svizzera di soccorso
Ringier	Ringier SA Ringier AG
santésuisse	Les assureurs-maladie suisses Die Schweizer Krankenversicherer
Scienceindustries suisse / Scienceindustries Switzerland	Wirtschaftsverband Chemie Pharma Life Sciences
SDV	Schweizer Dialogmarketing Verband
senesuisse	Association d'établissements économiquement indépendants pour presonnes âgées Suisse Verband wirtschaftlich unabhängiger Alters- und Pflegeeinrichtungen Schweiz
SPA	Swiss Payment Association

Spitex suisse / Spitex Schweiz	Aide et soins à domicile suisse Dachverband der Schweizer Nonprofit-Spitex
SSMD / SSO	Société suisse des médecins-dentistes Società svizzera odontoiatri Swiss Dental Association
SSV/UVS	Schweizerischer Städteverband Schweizerische Zahnärzte-Gesellschaft Union des villes suisses Unione delle città svizzere
Stiftung für Konsumentenschutz	Stiftung für Konsumentenschutz
suisa	Coopérative auteurs et éditeurs de musique Genossenschaft der Urheber und Verleger von Musik Cooperativa degli autori ed editori di musica
Sunrise UPC	Sunrise UPC GmbH
suva	Schweizerische Unfallversicherungsanstalt
SWICO	Wirtschaftsverband der ICT- und Online-Branche
Swimag	Swimag GmbH
Swiss Insights	Swiss Data Insights Association
SwissFoundations	Association of swiss grant-making foundations Association des fondations donatrices suisses Verband der Schweizer Förderstiftungen Associazione delle fondazioni donatrici svizzere
SwissHoldings	Verband der Industrie-und Dienstleistungsunternehmen in der Schweiz
swissICT	Fachverband ICT
swissprivacy.law	swissprivacy.law
swissstaffing	Verband der Personaldienstleister
thurbo	thurbo AG Regionalbahn
UBCS / VSKB	Union des Banques Cantonales Suisses Verband Schweizerischer Kantonalbanken Union delle Banche Cantonali Svizzere
UPS / SAV	Union patronale suisse UPS Schweizerischer Arbeitgeberverband SAV Unione svizzera degli imprenditori USI
UPSA / AGVS	Union professionelle suisse de l'automobile Auto Gewerbe Verband Schweiz Unione professinale svizzera dell'automobile
UPSV / SFF	Union Professionelle Suisse de la Viande Schweizer Fleischfachverband Svizzera della Carne
usam / sgv	Union suisse des arts et métiers Schweizerischer Gewerbeverband Unione svizzera delle arti e mestieri

USS / SGB	Union syndicale suisse Schweizerischer Gewerkschaftsbund Unions sindicale svizzera
UTP / VöV	Union des transports publics Verband öffentlicher Verkehr Unione dei transporti pubblici
veb.ch	Verband für Rechnungslegung, Controlling und Rechnungswesen
vsi	Verband Schweizerischer Inkassotreuhandinstitute
VUD	Verein Unternehmens-Datenschutz
Walderwyss	Walder Wyss AG

Tribunaux de la Confédération / Eidgenössische Gerichte / tribunali federali

TAF / BVGer	Tribunal administratif fédéral Bundesverwaltungsgericht Tribunale amministrativo federale

Renonciation à une prise de position / Verzicht auf Stellungnahme / Rinuncia a un parere

- JU, ZG, NE, TI
- Conférence des gouvernements cantonaux (CdC)
Konferenz der Kantonsregierungen (KdK)
- Union Démocratique Fédérale UDF
Eidgenössisch-Demokratische Union EDU
Unione Democratica Federale UDF
- Ensemble à Gauche EAG
- Parti évangélique suisse PEV
Evangelische Volkspartei der Schweiz EVP
Partito evangelico svizzero PEV
- Parti vert'libéral Suisse pvl
Grünliberale Partei Schweiz glp
Partito verde liberale svizzero pvl
- Lega dei Ticinesi (Lega)
- Parti suisse du travail PST
Partei der Arbeit PDA
- Association des Communes Suisses
Schweizerischer Gemeindeverband
Associazione dei Comuni Svizzeri
- Groupement suisse pour les régions de montagne
Schweizerische Arbeitsgemeinschaft für die Berggebiete
Gruppo svizzero per le regioni di montagna
- Union patronale suisse
Schweizerischer Arbeitgeberverband
Unione svizzera degli imprenditori

- Union suisse des paysans (USP)
  Schweiz. Bauernverband (SBV)
  Unione svizzera dei contadini (USC)
- Société suisse des employés de commerce
  Kaufmännischer Verband Schweiz
  Società svizzera degli impiegati di commercio
- Travail.Suisse
- Tribunal pénal fédéral
  Bundesstrafgericht
  Tribunale penale federale
- Tribunal fédéral suisse
  Schweizerisches Bundesgericht
  Tribunale federale svizzero
- Union patronale suisse
  Schweizerischer Arbeitgeberverband
  Unione svizzera degli imprenditori
- Comité international de la Croix-Rouge
- Associazione consumatrici e consumatori della Svizzera italiana ASCI
- Schweizerisches Konsumentenforum kf