Association SWISSPRIVACY
info@swissprivacy.law

Département fédéral de justice et police
Palais fédéral ouest
3003 Berne
Par courriel à :
Jonas.amstutz@bj.admin.ch

Lausanne, le 12 octobre 2021

Projet de révision totale de l'ordonnance relative à la Loi fédérale sur la protection des données

Madame la Conseillère fédérale,
Mesdames, Messieurs,

Dans le délai imparti au 14 octobre 2021, l'association SWISSPRIVACY a le plaisir de participer spontanément à la consultation du projet de révision totale de l'ordonnance relative à la nouvelle Loi fédérale du 25 septembre 2020 sur la protection des données[1].

Chapitre 1 Dispositions générales
Les art. 1 à 12 P-OLPD contiennent des dispositions générales relatives aux art. 1 à 18 nLPD. À ce sujet, les remarques suivantes peuvent être émises.

Corolaire du principe de sécurité de l'art. 8 nLPD, les art. 1 à 5 P-OLPD prescrivent les exigences minimales en matière de sécurité que tout responsable du traitement doit respecter. Le responsable du traitement qui ne respecte pas ces exigences minimales réalise une infraction pénale, passible d'une amende dont le plafond est fixé à CHF 250'000.– (art. 61 let. c nLPD). Or le P-OLPD ne définit pas avec la précision nécessaire les mesures techniques et organisationnelles à mettre en œuvre dont la violation aurait pour effet de faire entrer en jeu la responsabilité pénale du responsable du traitement. Il apparaît ce faisant contraire au principe de légalité auquel le droit pénal obéit (art. 1 CP).

Les conditions relatives à l'obligation de journalisation prévue à l'art. 3 P-OLPD diffèrent selon si le responsable du traitement est une personne privée ou un organe fédéral. Dans le premier cas, l'obligation de journalisation s'applique en cas de risque résiduel élevé (art. 3 al. 1 P-OLPD), alors que dans le second cas, l'obligation de journalisation s'applique en cas de traitement automatisé (art. 3 al. 2 P-OLPD). Cette distinction ne doit pas être maintenue dans la version finale de l'OLPD. L'obligation de journalisation doit être limitée aux cas représentant un risque résiduel élevé.

Les art. 6 et 7 P-OLPD précisent les prescriptions légales quant à la sous-traitance de données personnelles ancrée à l'art. 9 nLPD. L'art. 6 al. 2 P-OLPD dispose que, lorsqu'un sous-traitant n'est pas soumis à la nLPD, le responsable du traitement s'assure que d'autres dispositions légales garantissent une protection équivalente. Cette disposition nous interpelle dès lors que le champ d'application territorial tel que fixé à l'art. 3 nLPD repose sur le critère des effets, celui-ci étant relativement large. Dès lors que le sous-traitant d'un responsable du traitement traite *de facto* des données personnelles de personnes résidant en Suisse, nous ne voyons pas dans quel cas un sous-traitant n'est pas soumis à la nLPD. Nous recommandons ainsi sa suppression. Par ailleurs, l'art. 6 al. 3 P-OLPD oblige l'organe fédéral, en sa qualité de responsable du traitement, d'approuver par écrit la sous-traitance de deuxième rang. Selon nous, seuls les organes fédéraux soumis à la Directive (UE) 2016/680[2] devraient être soumis à cette obligation.

[1] nLPD ; FF 2020 7397.
[2] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Les art. 8 à 12 P-OLPD précisent les prescriptions légales liées à la communication de données personnelles à l'étranger des art. 16 à 18 nLPD. L'art. 8 P-OLPD diffère de l'art. 16 nLPD en ce sens qu'il prévoit en plus de l'État et de l'organisme international qu'un territoire ou une section déterminée dans un État peut se voir considérer comme ayant un niveau de protection adéquat. Cette précision nous surprend, dès lors que la nLPD ne le prévoit pas à proprement parler, raison pour laquelle nous recommandons sa suppression. En ce qui concerne le respect des droits humains, ce critère n'est pas pertinent et devrait également être supprimé. Finalement, nous soulignons que la procédure d'évaluation n'est pas réglée, en particulier le processus selon lequel un État pourrait demander une décision d'adéquation et si celle-ci est sujette à recours. Il convient ainsi de préciser ces éléments.

Nous relevons à ce stade que le P-OLPD ne précise pas l'art. 14 nLPD relatif au représentant, disposition ajoutée par l'Assemblée fédérale. À ce sujet, il nous semble utile de préciser dans la version finale de l'OLPD l'absence de responsabilité subsidiaire du représentant, qui pourrait notamment découler de l'obligation de tenir un registre. Les modalités de sa désignation et de ses connaissances doivent également être précisées, à l'instar de celles concernant le conseiller à la protection des données.

Chapitre 2 Obligations du responsable du traitement et du sous-traitant
Les art. 13 à 19 P-OLPD complètent les art. 19 à 24 nLPD relatifs aux obligations du responsable du traitement et du sous-traitant. Plusieurs dispositions nous interpellent.

L'art. 14 P-OLPD prévoit une disposition particulière relative au devoir d'informer des organes fédéraux lors de la collecte des données personnelles. Cette disposition ne nous semble pas nécessaire, dès lors que le caractère facultatif doit être indiqué dans tous les cas et pas uniquement en cas de recours à un questionnaire.

L'art. 16 P-OLPD prévoit que le responsable du traitement informe sans délai les destinataires auxquels il a communiqué des données personnelles de la rectification, de l'effacement ou de la destruction, ainsi que de la limitation du traitement des données personnelles. Selon nous, les obligations fondées sur l'art. 16 P-OLPD devraient être limitées dans le temps. Il devrait en outre être précisé que ces obligations ne fondent pas un devoir pour le responsable du traitement de conserver une copie des données communiquées et des destinataires y relatifs.

L'art. 18 P-OLPD prévoit que le responsable du traitement consigne par écrit l'analyse d'impact relative à la protection des données personnelles, en tous les cas pendant deux ans après la fin du traitement des données. Imposer la forme écrite ne nous semble pas justifié et l'analyse d'impact relative à la protection des données devrait pouvoir être établie et conservée sous forme électronique. Bien qu'il découle du Rapport explicatif relatif à la procédure de consultation que la forme écrite comprend la forme électronique (cf. p. 24), il nous paraît essentiel de rappeler que la forme écrite exige une signature (TAF A-3548/2018 du 19 mars 2019, consid. 4.8.4). Dès lors, si la forme écrite devait être maintenue, elle doit être comprise de manière plus large que la règle formelle des art. 12 ss CO. Ce point doit être spécifiquement prévu (il en va de même en ce qui concerne l'art. 20 P-OLPD). En outre, il nous semble que le recours à la notion de « traitement » pourrait conduire à une conservation relativement longue, dès lors qu'il est admis que l'archivage de données est un traitement (art. 5 let. d nLPD).

L'art. 19 P-OLPD prévoit les modalités liées à l'annonce des violations de la sécurité des données et concrétise l'art. 24 nLPD. Afin de gagner en précision, l'al. 1 pourrait préciser que cet alinéa s'applique « en cas d'annonce obligatoire de violations de la sécurité des données », et non lors de toute violation. Le responsable du traitement qui voudrait informer le PFPDT de manière volontaire ne devrait ainsi pas forcément donner toutes les informations listées à l'al. 1. Concernant la notification échelonnée, elle est bienvenue. Il pourrait cela étant être utile de préciser si cela constitue bel et bien une possibilité (« peut » ; *kann*), et non une obligation (à l'instar de l'art. 33 par. 4 RGPD[3], malgré le texte imprécis qui semble indiquer une simple possibilité). Enfin, alors que la nLPD ne prévoit pas de telle obligation, nous sommes étonnés de découvrir une obligation, reprise du droit de l'Union européenne, de documenter les violations (al. 5). Cette obligation, qui ne découle pas d'une délégation législative, n'est pas valable et donc inefficace. Elle devrait ainsi être supprimée. Elle est en outre imprécise, car il n'est pas clair, comme pour l'al. 1, si, aux yeux de l'Office fédéral de la justice, cette obligation aurait dû viser toutes

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

les violations (comme à l'art. 33 par. 5 RGPD) ou uniquement celles qui doivent être annoncées au PFPDT.

Chapitre 3 Droits de la personne concernée
Les art. 20 à 24 P-OLPD complètent les art. 25 à 29 nLPD relatifs aux droits des personnes concernées. Nous relevons ce qui suit.

Les art. 20 ss P-OLPD concernent les modalités liées au droit d'accès. L'art. 20 al. 1 P-OLPD, ainsi que l'art. 20 al. 2 P-OLPD précisent que la demande de renseignement peut être faite par écrit (sauf exception), de même que l'envoi des renseignements. En lien avec notre commentaire relatif à l'analyse d'impact relatif à la protection des données, l'exigence de la forme écrite (et des règles formelles qui en découlent) ne se justifie pas. La forme électronique, et ses exigences, doivent être expressément prévues. En outre, l'art. 20 al. 2 P-OLPD dispose que d'entente avec le responsable du traitement, ou sur sa proposition, la personne concernée peut consulter ses données sur place. Selon nous, la consultation sur place doit pouvoir avoir lieu indépendamment de savoir qui l'a proposée. L'art. 20 al. 5 P-OLPD prévoit que le responsable du traitement documente le motif pour lequel il refuse, restreint ou diffère la communication des informations. Ce devoir de documentation ne découle pas de la nLPD et pourrait sortir du cadre des art. 25 ss nLPD. Finalement, la terminologie (« informations », « renseignements ») pourrait être uniformisée.

L'art. 22 al. 1 P-OLPD dispose que les renseignements, ou les causes de la restriction, sont fournis dans les 30 jours suivants réception de la demande. Il semble important de préciser que ce délai de 30 jours court dès la réception de la demande ou de la confirmation de l'acceptation des frais. À ce sujet, l'art. 23 al. 3 P-OLPD prévoit que la personne concernée doit être préalablement informée du montant des frais et se voir la possibilité de retirer sa requête dans les dix jours. La personne concernée ne devrait pas seulement pouvoir retirer sa demande, mais il devrait également être prévu qu'elle puisse confirmer sa demande en acceptant les frais potentiels. Dans la pratique, l'absence de réponse est problématique puisque le responsable du traitement doit déployer des efforts disproportionnés sans obtenir de garantie quant au paiement. Toutefois, il serait contraire à l'essence du droit d'accès de subordonner le paiement des frais à l'envoi des informations.

L'art. 12 al. 5 nLPD dispose que « [l]e Conseil fédéral prévoit des exceptions pour les entreprises qui emploient moins de 250 collaborateurs et dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées ». La concrétisation de cette délégation expresse reste trop vague et manque le but d'atteindre une certaine sécurité juridique. Le rapport explicatif mentionne pourtant un « catalogue » (p. 12), que l'on peine à retrouver à l'art. 26 P-OLPD.

Chapitre 4 Dispositions particulières pour le traitement de données personnelles par des personnes privées
Les art. 27 à 45 P-OLPD contiennent des dispositions particulières pour le traitement de données personnelles par des organes fédéraux et complètent les art. 33 à 59 nLPD. Nous relevons à ce propos ce qui suit.

L'art. 42 P-OLPD prévoit que le PFPDT peut transmettre les informations relatives à l'annonce d'une violation de la sécurité des données au NCSC afin qu'il analyse l'incident. La personne responsable de l'annonce doit toutefois donner son accord. La notion de « responsable du traitement » devrait être favorisée à celle de « personne responsable de l'annonce », qui se rapproche de la notion de personne tenue d'annoncer de l'art. 24 al. 6 nLPD.

Veuillez croire, Madame la Conseillère fédérale, Mesdames, Messieurs, à l'expression de notre parfaite considération.

Le Comité de l'association SWISSPRIVACY