FÉDÉRATION ROMANDE DES CONSOMMATEURS
LE POUVOIR D'AGIR

Département fédéral de justice
et police
Office fédéral de la justice

Envoyé par mail à
jonas.amstutz@bj.admin.ch

Lausanne, le 6 octobre 2021

Consultation sur la révision totale de l'ordonnance relative à la Loi fédérale sur la protection des données (OLPD)

Monsieur,

La Fédération romande des consommateurs (FRC) vous remercie de l'avoir associée à la consultation sur la révision totale de l'ordonnance relative à la Loi fédérale sur la protection des données (OLPD).

Les consommateurs de Suisse sont au centre des problématiques liées à la protection des données. L'asymétrie informationnelle, l'opacité des pratiques de collecte et d'exploitation des données personnelles, les incertitudes liées aux modalités de stockage de même que les risques de piratage rendent ces dispositions légales cruciales.

Notre association a activement pris part aux débats concernant la révision de la Loi sur la protection des données et, malgré certaines améliorations, regrette que les pouvoirs du Préposé fédéral n'aient pas été davantage renforcés, que les sanctions restent dérisoires et que la problématique du profilage à des fins de solvabilité n'ait pas été réglée[1].

Vous trouverez ci-après nos remarques en lien avec les points qui touchent directement les consommateurs.

[1] https://www.frc.ch/protection-des-donnees-lavenir-seclaircit-un-peu/

Fédération romande des consommateurs
Rue de Genève 17, Case postale 6151
1002 Lausanne
Tél. 021 331 00 90
info@frc.ch, www.frc.ch

Personne de contact
Marine Stücklin
Responsable Droit et Politique
m.stuecklin@frc.ch

Exigences minimales en matière sécurité des données (art. 8ss nLPD; art. 1ss P-OLPD)
Selon le nouvel article 61, let. c nLPD, celui qui ne respecte pas, intentionnellement, les exigences minimales en matière de sécurité des données édictées par le Conseil fédéral s'expose à une amende de 250 000 francs au plus (art. 61, let. c nLPD). Il est essentiel que le Conseil fédéral ne vide pas cette disposition de sa portée en prévoyant des mesures trop modestes ou trop peu claires.

En l'état, le projet ne permet pas de déterminer avec suffisamment de précision ce qui entrainerait l'application de la disposition pénale. En effet, l'utilisation de notions juridiques indéterminées dans cette section 1 est très regrettable car elle affaiblit l'étendue de la protection ainsi que la possibilité de recourir à la disposition pénale («A des intervalles appropriés», art. 1, al. 2 P-OLPD ; «Dans la mesure du possible», art. 2 P-OLPD); il convient d'y renoncer. La fréquence à laquelle les mesures doivent être réexaminées doit également être clairement indiquée dans l'ordonnance (art. 1 , al. 2 P-OLPD), toute marge d'interprétation et d'appréciation dans ce domaine risquant de porter atteinte à la sécurité des données.

Journalisation (art. 3 P-OLPD)
La journalisation doit permettre de vérifier le traitement des données personnelles *a posteriori*, afin de déterminer si des données ont été perdues, effacées, détruites, modifiées ou si elles ont été divulguées. Cette obligation joue donc un grand rôle en matière de sécurité. Néanmoins, la journalisation implique de fournir des informations sur la nature du traitement, l'identité de la personne qui a effectué le traitement, l'identité du destinataire et le moment auquel le traitement a eu lieu, etc. Elle peut donc représenter un risque de surveillance des personnes concernées, lequel est justifiable si le traitement envisagé présente un risque élevé pour la personnalité ou les droits fondamentaux. Aussi, le fait que la journalisation ne doit être effectuée que de manière subsidiaire, après une pesée des intérêts, devrait davantage ressortir du texte de l'art. 3 P-OLPD.

La journalisation ne devrait au surplus pas dépendre strictement des résultats de l'analyse d'impact. En effet, le responsable du traitement peut être délié de son obligation d'établir une analyse d'impact s'il soumet un code de conduite au PFPDT (art. 22, al. 5 nLPD) mais n'est pas forcé de le modifier s'il donne lieu à une prise de position critique du PFPDT (art. 11, al. 2 nLPD). Il en découle que tous les cas où les traitements envisagés présentent un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées doivent faire l'objet d'une journalisation, indépendamment de la tenue ou non d'une analyse d'impact.

Communication de données personnelles à l'étranger (art. 16ss nLPD; art. 8ss P-OLPD)
L'art. 8, al. 1 P-OLPD pose les critères qui doivent être pris en compte pour évaluer l'adéquation du niveau de protection de l'Etat de destination. Parmi les conditions figure le respect des droits humains (art. 8, al. 1, let. b P-OLPD). Bien que louable, ce critère ne semble pas suffisamment clair en tant que tel pour être pertinent. Il conviendrait 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.

De manière générale, la possibilité d'octroyer une autorisation lorsqu'un secteur déterminé d'un Etat accorde un niveau de protection suffisant doit être conditionné au fait que le secteur déterminé n'est pas assujetti aux lois ou à certaines des lois de l'Etat 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. Ces critères devraient figurer dans l'ordonnance.

En l'absence de décision du Conseil fédéral, l'art. 16, al. 2 nLPD prévoit que les données personnelles peuvent être communiquées à l'étranger si un niveau de protection approprié est garanti notamment par un contrat conclu entre le responsable du traitement ou le sous-traitant et son cocontractant. Le PFPDT est informé. Dans ces cas et malgré les clauses de protection de données impératives listées à l'art. 9, al. 1 P-OLPD, nous jugeons grand le risque que ledit contrat et partant, le niveau de protection des données, ne soient jamais respecté dans certains pays.

De plus, au vu de l'expérience du « Swiss-U.S. Safe Harbor Framework », remplacé par le « Swiss-U.S. Privacy Shield Framework », lui-même ensuite révoqué, il semble illusoire de considérer qu'une telle entente puisse offrir une protection suffisante vis-à-vis de la primauté de l'intérêt d'Etat dans de nombreux pays.

Enfin, il nous paraît important de repréciser dans l'ordonnance que la communication de données à l'étranger doit respecter le niveau de protection de la nLPD.

Devoir d'informer (art. 19ss nLPD; 13ss P-OLPD)
Nous saluons les articles 13, al. 1 et 15 P-OLPD, lesquels précisent que les informations sur la collecte des données personnelles doivent être communiquées de manière concises, compréhensible et facilement accessibles et que les données personnelles communiquées sont actuelles, fiables et exhaustives. Ce n'est que de cette manière qu'une personne pourra se déterminer sur ses données et exercer ses droits.

Il est également essentiel que la personne concernée soit informée sans délai de la rectification, de l'effacement ou de la destruction de ses données pour s'assurer que ses instructions ont bien été suivies d'effet (art. 16 P-OLPD).

Décision automatisée (art. 21 nLPD; art. 17 P-OLPD)
Les décisions automatisées peuvent être injustes et une personne qui demande la réévaluation de sa demande par une personne physique ne doit pas être désavantagée pour ces motifs. Notre association salue donc cette disposition.

Droit d'accès (art. 25ss nLPD; 20ss P-OLPD)
Le droit d'accès figure parmi les droits les plus importants de la personne concernée et il est important de veiller à ce que son exercice ne soit pas rendu inutilement compliqué. A cet égard, une demande envoyée par mail avec preuve de l'identité doit pouvoir suffire.

La FRC salue en particulier l'art. 21 P-OLPD qui permet à la personne concernée d'adresser sa demande auprès de chaque responsable du traitement sans avoir à rechercher la personne compétente. Le délai de traitement d'une demande d'accès ne doit, dans tous les cas, pas excéder un délai de 30 jours (art. 22, al. 1 P-OLPD).

Concernant les exceptions à la gratuité (art. 23, P-OLPD), le fait de demander une participation équitable aux frais ne doit pas devenir un moyen pour les responsables de traitement de dissuader les personnes concernées d'avoir accès à leurs données. Pour cette raison, il convient d'ajouter «A titre exceptionnel» au début de l'alinéa 1 pour souligner le fait qu'une participation financière ne peut être demandée que dans de rares cas. Par ailleurs, le responsable du traitement, en plus de chiffrer le coût extraordinaire, devrait expliquer ce qui les justifie. En d'autres termes, il doit indiquer en quoi la demande occasionne des efforts disproportionnés. Dans la mesure où leurs obligations légales sont connues, les responsables du traitement

doivent s'organiser en amont pour qu'une demande d'accès soit facilement réalisable et que lesdits «efforts disproportionnés» restent rares.

Enfin, le responsable du traitement doit obtenir une confirmation de la part de la personne concernée avant de continuer à traiter sa demande, une absence de réaction ne devant en aucun cas pouvoir être interprétée comme un consentement aux frais (art. 23, al. 3 P-OLPD). L'obtention d'une confirmation écrite permettra par ailleurs d'éviter un travail inutile du responsable du traitement.

Exception à l'obligation de tenir un registre des activités de traitement (art. 12, al. 5 nLPD; art. 26 P-OLPD)
Notre association regrette beaucoup que les entreprises de moins de 250 employés (c'est-à-dire plus de 99% des entreprises en Suisses[2]) soient exemptées de l'obligation de tenir un registre des activités de traitement. Alors même que la protection des données constitue un enjeu majeur pour les PME qui traitent un volume de données personnelles toujours plus important et sont, conséquemment, parmi les cibles privilégiées des hackers. La tenue d'un registre constitue ainsi est un moyen simple pour permettre au responsable du traitement de s'assurer qu'il respecte bien ses obligations en matière de protection des données.

Le fait de vouloir limiter cette exception est bienvenu mais 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 (art. 26 P-OLPD). On se demande même si le fait de traiter de données sensibles ne devrait pas, en soi, constituer une telle exception sans qu'il soit nécessaire d'être face à un traitement « à grande échelle ».

Notions qui mériteraient un développement
De manière plus générale, on s'étonne que la ***notion de profilage à risque élevé*** (art. 5, let. g nLPD) ne soit pas davantage développée dans l'ordonnance dans la mesure où il s'agit d'une notion nouvelle, élaborée ex nihilo et ayant fait l'objet d'un large débat entre les deux Conseils. Il en va de même pour le concept de ***protection des données dès la conception et par défaut*** (art. 7 nLPD) qui ne fait l'objet d'aucune précision. Il conviendrait de mieux le définir, comme le fait le Règlement (UE) 2016/679 du 27 avril 2016 sur la protection des données dans son paragraphe introductif §78.

En vous remerciant de prendre en compte notre position, nous vous prions de recevoir, Monsieur, nos salutations les meilleures.

Fédération romande des consommateurs

Sophie Michaud Gigon
Secrétaire générale

Marine Stücklin
Responsable Droit et Politique

[2] https://www.bfs.admin.ch/bfs/fr/home/statistiques/industrie-services/entreprises-emplois/structure-economie-entreprises/pme.html