canton de vaud
LIBERTÉ ET PATRIE

CONSEIL D'ETAT

Château cantonal
1014 Lausanne

Madame la Conseillère fédérale
Karin Keller-Sutter
Cheffe du Département fédéral de justice
et police (DFJP)
3003 Berne

Par courrier électronique à :
jonas.amstutz@bj.admin.ch

Réf. : 21_COU_7296

Lausanne, le 13 octobre 2021

Réponse du Canton de Vaud à la consultation fédérale sur le projet de révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (P-OLPD)

Madame la Conseillère fédérale,

Le Conseil d'Etat a pris connaissance du projet de révision totale de l'ordonnance relative à la loi fédérale du 15 septembre 2020 sur la protection des données et vous remercie de l'avoir consulté à ce sujet.

Convaincu de la nécessité impérieuse de protéger les personnes, les entreprises et autres collectivités des risques découlant d'une utilisation abusive de leurs données, ainsi qu'il l'a affirmé dans sa Stratégie numérique de novembre 2018, le Conseil d'Etat ne saurait, en l'état, soutenir le projet de révision mis en consultation, dès lors que bon nombre de ses dispositions et notamment celles qui portent sur la sécurité des données, manquent à ce stade de la clarté qui permettrait aux responsables privés ou fédéraux de traitement des données de les mettre en œuvre. Dans ce contexte, le Conseil d'Etat note qu'à ce stade, le projet de révision reprend des termes et dispositions obsolètes de l'ordonnance fédérale précédente, et, de manière partielle, certaines dispositions du 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 (RGPD), ne permettant pas d'en saisir la finalité.

Pour le Conseil d'Etat, il est indispensable que la future ordonnance soit précise car la loi fédérale est complexe, contient de nombreuses normes de délégation, et introduit des concepts nouveaux tels que celui du profilage à risque élevé (article 5 let g nLPD). Le Conseil d'Etat est d'ailleurs d'avis que toute forme de profilage est en soi un traitement de données à risque élevé, susceptible de porter atteinte à la personnalité ou aux droits fondamentaux d'une personne. Enfin, le Conseil d'Etat rappelle que la nLPD et l'OLPD serviront de référence au droit cantonal de la protection des données que les cantons devront réviser notamment pour tenir compte des évolutions sociétales et techniques, ainsi que de certaines dispositions du droit européen – il est dès lors essentiel que le droit fédéral soit précis.

Le Conseil d'Etat demande ainsi au Conseil fédéral de clarifier le projet de révision, en tenant compte de ses commentaires figurant en annexe.

En vous remerciant de l'attention que vous porterez à la présente détermination, le Conseil d'Etat vous prie de croire, Madame la Conseillère fédérale, à l'assurance de sa haute considération.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE	LA CHANCELIERE a.i.
Nuria Gorrite	Sandra Nicollier

Annexe mentionnée

Copies

- Autorité de protection des données et de droit à l'information
- Office des affaires extérieures

Annexe

Commentaires article par article :

Section 1 sécurité des données

D'une manière générale, le P-OLPD ne précise pas suffisamment les exigences minimales en matière de sécurité des données (art. 8 nLPD) et ne permet pasde reconnaitre les éléments objectifs de l'infraction relative à la violation des devoirs de diligence (art. 61 al. 1 let. c nLPD).

En effet, le P-OLPD s'en tient au concept de l'ordonnance précédente et le complète par des termes de droit européen, sans préciser la nécessité d'adapter les mesures visant à sécuriser les données à la finalité de leur traitement ainsi qu'aux outils utilisés. Dans ce contexte, il pourrait être pertinent de prévoir de se référer à des normes techniques et organisationnelles internationalement reconnues, qui permettraient de tenir compte des évolutions technologiques.

Il serait également nécessaire par ailleurs de fixer dans cette section des critères indiquant la pertinence voire l'obligation de conduire des analyses d'impact de protection des données (DPIA). En effet, il s'agit 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 LPD.

Article 1

L'al. 1 semble reprendre pour l'essentiel l'art. 32 du RGPD sans toutefois se concentrer sur l'objectif formulé dans cet article, à savoir : « assurer un niveau de protection adapté au risque ». Cela signifie, qu'en fonction des cas, il conviendra au préalable d'évaluer les objectifs, les besoins et les risques en matière de protection des données. A ce sujet, les objectifs de protection sont déjà fixés à l'art. 5 al. 1 let. h nLPD, comme le mentionnent également les notes explicatives (p. 15 du rapport), et sont énumérés en détail à l'art. 2 P-OLPD (voir ci-dessous art. 2 P-OLPD). Le besoin de protection est déterminé par le type de données (données personnelles, données personnelles sensibles) et le traitement des données en lui-même (par exemple, le profilage). Ce n'est qu'ensuite qu'aura lieu l'évaluation des risques, comme le prévoit également l'analyse d'impact sur la protection des données (art. 22 nLPD).
Les critères « finalité, nature, étendue et circonstances du traitement des données » se réfèrent ainsi à l'évaluation du besoin de protection (qui contient déjà une première estimation approximative de l'étendue possible du dommage), les critères « probabilité de survenance et d'impact potentiel sur les personnes concernées » à l'évaluation des risques. Lorsqu'il s'agit d'évaluer l'adéquation des mesures, les critères « état de la technique et coûts de mise en œuvre » semblent pertinents. Toutefois, ils ne renseignent qu'indirectement sur l'opportunité d'une mesure, car en ce qui concerne cette dernière, il faut avant tout permettre d'évaluer si une mesure doit être prise et, concrètement, laquelle permet de contrer le risque de manière adéquate (cf. art. 32 RGPD et notes explicatives, p. 15).

L'art. 1 al. 1 P-OLPD devrait donc être entièrement revu sur le plan conceptuel et il serait judicieux d'ajouter, à la lettre a) les critères de **profilage**, de **transferts internationaux** et de **sous-traitance** (Cloud). Ces situations sont particulièrement critiques en matière de gestion des risques, tant pour les personnes physiques que morales.

L'al. 2 exige que les mesures soient examinées à intervalles appropriés pendant toute la durée du traitement. Cette formulation apparaît insuffisante en ce sens que l'évaluation des risques dont découle les mesures et leur pertinence, doit être revue en permanence et par conséquent induire l'adaptation éventuelle des mesures. Cet alinéa devrait être reformuler afin de garantir une sécurité suffisante des données.

Le Conseil d'Etat propose d'ajouter à cet article un troisième alinéa ayant la teneur suivante :

Art. 1, al. 3 [Nouveau] *: « Le PFPDT publie des recommandations sur les mesures techniques et organisationnelles que le responsable du traitement et les sous-traitants peuvent envisager selon la nature des données personnelles traitées »*.

En effet, l'élaboration de « recommandations de bonne pratique », sous l'égide du PFPDT, sur les moyens que le responsable du traitement peut mettre en œuvre, avec des exemples concrets d'application (p. ex. dans le domaine médical) pourrait servir de référence aux exigences à remplir et à l'évaluation cas échéant (p. ex. les autorités de surveillance ou la justice). Cette proposition va également dans le sens du Commentaire § 4.1.1 « Sécurité des données » p. 14, troisième paragraphe, qui précise : « En toute logique, les exigences sont plus élevées pour un hôpital qui traite régulièrement des données sensibles que pour une boulangerie ou une boucherie qui traite les données de ses clients ou de ses fournisseurs. »

Article 2

Les exigences énumérées ne représentent pas des objectifs de protection indépendants, mais plutôt des exigences relatives aux mesures à prendre pour atteindre les objectifs de protection (par exemple, le contrôle d'accès ne représente pas un objectif de protection, mais plutôt une exigence visant à garantir la confidentialité dans le cadre du principe de proportionnalité). Si l'art. 5 al. 1 let h nLPD énumère ces objectifs de protection, il serait opportun de les détailler plus clairement dans l'ordonnance d'application tout en actualisant et harmonisant les termes.
En outre, il conviendrait de préciser dans la phrase introductive de l'art. 2 que les mesures devraient être définies en tenant compte des risques identifiés lors de l'évaluation des risques, et porter sur les éléments listés dans l'article.

Article 3

L'objectif de la journalisation est que, dans les cas où le traitement non autorisé de données personnelles ne peut pas être techniquement exclu dès le départ, il puisse être ultérieurement déterminé (et sanctionné dans certaines circonstances par la suite) lors de l'analyse du journal. La journalisation résulte donc de l'évaluation des risques et de la planification des mesures. Il doit s'agir d'un moyen approprié au regard d'un risque concret

qui peut être efficacement réduit par la journalisation (proportionnalité du nouveau traitement des données). L'obligation de journalisation des données en tant que mesure compensatoire ne devrait donc s'appliquer que dans les cas où elle répond effectivement à un risque identifié.

L'al. 2 prévoit que pour les organes fédéraux, la journalisation doit s'appliquer au traitement de toutes les données personnelles. Cette mesure paraît aller trop loin, et être trop contraignante. La journalisation constitue en soi une acquisition de données personnelles, qui doit satisfaire au principe de proportionnalité. Il est vrai que l'art. 57 let. b ch. 4 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA) permet l'enregistrement de données marginales dans le but de tracer l'accès aux collections de données, mais seulement dans la mesure où l'enregistrement est proportionné. Le fait que, même dans le cas de données personnelles simples et même avec des autorisations restrictives, chaque accès en lecture doive être enregistré va clairement au-delà de cette exigence. L'obligation des organes fédéraux de « journaliser » ne doit pas aller plus loin que celle des personnes privées responsables du traitement. Il conviendrait donc d'inclure les organes fédéraux dans l'al. 1 et de supprimer l'al. 2.

Al. 3, il convient d'insérer les mots "**le cas échéant**" avant "l'identité du destinataire", car tout traitement enregistré ne constitue pas une divulgation.

Al. 4, les journaux doivent être conservés pendant deux ans et ne peuvent être utilisés que pour contrôler les règles de protection des données ou pour rétablir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données. Dans ce contexte, une évaluation liée à la personne n'est pas nécessaire dans tous les cas (cf. art. 57m et suivants LOGA et ATF 143 II 443 qui précisent les modalités des évaluations et des procédures échelonnées) pour les organes fédéraux. Il convient donc de modifier la dernière phrase comme suit : « **ne peuvent être utilisés qu'à cette fin et dans la mesure nécessaire à l'égard des personnes** ».

Article 4

Avec cette nouvelle norme, la protection des particuliers s'amoindrit. En effet, l'al. 1 restreint de façon arbitraire l'obligation de créer un règlement de traitement pour les responsables privés et leurs sous-traitants mandatés. Cette solution limitée à deux cas de figure ne permet plus de garantir les droits de la personne concernée dans le traitement de ses données.
Il convient ici de reprendre les exigences de l'analyse d'impact sur la protection des données (cf. art. 22 al. 1 nLPD). Dans le cadre de l'analyse d'impact sur la protection des données, de nombreux documents sont également créés (art. 22 al. 3 nLPD), qui peuvent faire partie du règlement de traitement. Les recommandations de bonne pratique évoquées plus haut permettraient également de garantir un cadre sécuritaire dès que le traitement porte sur des données sensibles que ce soit à grande échelle ou non.

L'al. 2 n'établit aucun lien avec les normes en matière de technologie de l'information auxquelles il conviendrait de se référer. Une solution simple serait de se référer aux exigences spécifiques de la protection des données (let. h, j).

L'al. 3 semble peu pratique. Le conseiller à la protection des données est le spécialiste du responsable du traitement et c'est lui qui élabore un ensemble de règles de traitement et veillera également à son actualisation cas échéant. La formulation « le met à la disposition du conseiller à la protection des données sous une forme qui lui est intelligible » implique manifestement une dévalorisation des compétences spécialisées requises (art. 10 al. 3 let. c nLPD). L'une des tâches du conseiller à la protection des données est d'aider à l'application de la réglementation en matière de protection des données (art. 10 al. 2 let. b nLPD). L'al. 3 P-OLPD devrait être supprimé sans être remplacé.

Article 5

cf. commentaire article 4.

Article 6

Correction d'une coquille à l'al. 3 « Lorsque le responsable **du** traitement … ».

Article 7

Le conseiller à la protection des données de l'organe fédéral doit également collaborer à l'application des dispositions relatives à la protection des données (cf. ci-dessous art. 28 P-OLPD). Il est contraire à l'approche préventive et axée 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 en cas de transfert de fonctions. Les tâches d'un conseiller en protection des données incluent la participation à de telles transactions ; il s'agit d'une tâche essentielle et le conseiller à la protection des données doit être informé en temps utile, comme cela est prévu lors de la conception de projets de traitement automatisé de données personnelles (art. 31 P-OLPD). L'art. 7 P-OLPD devrait être supprimé sans être remplacé.

Article 8

La mise en application de cet article impliquerait que le PFPDT soit consulté formellement alors que les appréciations des organisations internationales ou des autorités étrangères peuvent quant à elles être prises en compte matériellement. Il convient donc de préciser que les avis du PFPDT sont également à prendre en compte sur le plan matériel, d'autant que les notes explicatives ne se prononcent pas à ce sujet (notes explicatives, p. 27).

Article 9

En vertu de 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. La formulation introductive de l'al. 3 pourrait laisser penser que l'absence de communication, dans certains cas, constituerait également une divulgation conforme à la loi à l'étranger. 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. La formulation devrait être adaptée afin de lever toute ambiguïté.

Article 13

. L'article 13 pourrait préciser qui est responsable au premier chef de la communication sur le traitement de données entre le responsable de traitement et le sous-traitant, en garantissant une bonne coordination ainsi qu'une information uniforme et valable à la personne concernée.

Article 19

L'art. 24 al. 1 nLPD prévoit la notification des violations de sécurité des données uniquement dans les cas susceptibles d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. L'art. 24 al. 2 nLPD précise le contenu de la notification et énonce les exigences relatives à l'information des personnes concernées (art. 24 al. 4 et 5 nLPD).

L'art. 24nNLPD diverge de l'art. 33 RGPD ; cependant, la majorité des dispositions de l'art. 33 RGPD sont reprises pour l'essentiel dans l'art. 19 P-OLPD. Si ces dispositions sont utiles pour les contrôleurs qui sont également soumis au RGPD, ce n'est pas le cas pour la majorité des responsables du traitement. Cet article introduit des dispositions supplémentaires inutiles, souvent limitées par la formulation « dans la mesure du possible ». L'art. 24 nLPD n'a pas besoin de la concrétisation contenue dans l'art. 19 P-OLPD.

Article 20

Les art. 25 et 26 nLPD réglementent en détail le droit à l'information et ses restrictions ; les précisions fournies par l'art. 20 P-OLPD vont au-delà de ce qui est nécessaire.

L'al. 3 précise que les renseignements doivent être compréhensibles pour la personne concernée ; cette formulation est trompeuse car elle impliquerait que le responsable du traitement devrait traiter des données supplémentaires sur la personne qui demande des informations afin d'établir avec certitude sa bonne compréhension. Or le contenu de l'information est défini à l'art. 25 al. 2 nLPD qui détermine la portée et le but de l'information, mesuré selon des critères objectifs. Il importe que le droit à l'information puisse être intégré dans les processus du responsable du traitement comme une norme évidente de la loi sur la protection des données. L'art. 20 al. 3 P-OLPD devrait être supprimé sans être remplacé.

L'al. 4 rappelle inutilement l'obligation pour les responsables du traitement de « protéger les données de la personne concernée de tout accès de tiers non autorisé lors de la communication des renseignements ». Cette obligation découle déjà de l'art. 8 nLPD et des dispositions du chapitre 1 de P-OLPD. L'al. 4 P-OLPD devrait être modifié en ce sens.

L'al. 5 oblige le responsable du traitement à documenter la restriction et conserver cette documentation pendant au moins trois ans. Cette nouvelle obligation crée un travail supplémentaire sans garantie sur la suite donnée ni cadre précis sur la durée de conservation de ces informations partielles. Selon l'art. 26 al. 4 nLPD le responsable du traitement doit indiquer pourquoi il refuse, restreint ou reporte l'information ; cette disposition est suffisante pour que la personne concernée puisse faire valoir son droit à

l'information en justice si nécessaire. L'al. 5 P-OLPD devrait être supprimé sans être remplacé.

Article 21

L'al. 1 prévoit que le responsable du traitement qui n'est pas compétent pour traiter la demande doit la transmettre au responsable du traitement compétent. Ce principe de droit administratif s'applique aux organes fédéraux même sans être mentionné dans ce contexte. Si dans le domaine du droit public, cette obligation résulte de la relation souveraine des citoyens avec l'État, dans la relation de droit privé, en revanche, les parties déterminent leurs droits et obligations de manière autonome. Il est disproportionné d'imposer la même obligation à la personne responsable de droit privé. Elle conduit à un effort de recherche de la personne « responsable » en droit privé sans renforcer les droits des personnes concernées. L'al. 1 2ème phrase P-OLPD devrait être supprimé sans être remplacé.

Article 23

Cette disposition pourrait être complétée par un renvoi aux dispositions topiques de la législation sur la protection des données régissant la procédure à suivre lorsque la personne concernée conteste l'émolument demandé car, contrairement à l'organe saisi, elle estimerait par exemple que les efforts à déployer pour répondre à sa demande ne seraient pas disproportionnés.

Article 24

Se référer à l'application analogue des dispositions sur le droit d'accès pour la mise en œuvre de l'art. 28 nLPD ne rend pas justice à la nouvelle institution juridique de la « portabilité des données » et ne répond pas à la nécessité de la concrétiser. Il serait judicieux de traiter ici notamment des « formats électroniques communs » ou de « l'effort disproportionné » en cas de transfert direct d'un contrôleur de données à un autre. En outre, en ce qui concerne les exceptions de gratuité, une réglementation différente de celle du droit à l'information serait également concevable, car ici ce n'est pas la protection de la personnalité mais la valeur économique des données qui est au premier plan. L'art. 24 P-OLPD devrait ainsi être complètement révisé.

Article 25

La formulation de cet article paraît trompeuse et devrait être corrigée. En effet, aucune référence n'est faite à l'art. 10 al. 2 nLPD, qui énumère deux tâches du conseiller à la protection des données en particulier : la formation et le conseil ainsi que la participation à l'application des règles de protection des données. Ces obligations légales sont exhaustives, c'est pourquoi les obligations de l'art. 25 al. 1 let a et b P-OLPD ne sont pas les obligations que ce conseiller doit remplir, mais une simple concrétisation des obligations déjà énoncées à l'art. 10 al. 2 nLPD.

Article 26

Restreindre l'obligation de tenir un registre des activités de traitement qu'à deux situations très précises ne couvre pas les traitements de données qui sont essentiels pour les droits de la personne. Comme dans le cas de l'art. 4 al. 1 P-OLPD, ici aussi, il convient de reprendre les exigences relatives à l'analyse d'impact sur la protection des données (le traitement comporte un risque élevé pour la personnalité et les droits fondamentaux des personnes concernées ; art. 22 al. 1 nLPD).

Article 28

L'al. 2 omet de reprendre la tâche prévue à l'art. 10 al. 2 let. b nLPD – concourir à l'application des prescriptions relatives à la protection des données – seule figure la formation et le conseil de l'art. 10 al. 2 let. a nLPD. Il s'agit probablement d'un oubli, puisque la participation à l'application des réglementations en matière de protection des données est une tâche essentielle des conseillers à la protection des données. Cette tâche devrait ainsi être ajoutée à l'art. 28 al. 2 P-OLPD.

Article 33

Cette disposition devrait être complétée de manière à prévoir une obligation de consulter les autorités cantonales lorsque les projets les impliquent également.

Article 36

La disposition est superflue car cette spécification est déjà claire à partir de l'art. 39 nLPD.

Annexe relative à la modification de l'Ordonnance sur les relevés statistiques
Liste des statistiques (Ch. 72, titre, 3e ligne, 2e colonne, et 9e ligne, 2e colonne)

Il ressort de ce descriptif qu'« avec l'accord des intéressés, il est possible d'utiliser certaines informations dans certains buts administratifs », ce qui 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 est proposé de compléter par des exemples, ce que l'on entend par « dans certains buts administratifs », avec la mention « notamment » ou « tels »…

Traitement de données sensibles

Le Conseil d'Etat relève que le traitement de données sensibles devrait, selon la nLPD être prévu au niveau d'une base légale formelle. Or on peut constater dans les textes mis en consultation, l'introduction de normes autorisant le traitement de données sensibles. Ces dispositions devraient être retirées du projet de révision et être soumises dans un projet de loi aux Chambres fédérales.

Propositions rédactionnelles :

- No 109 (ordonnance sur le travail au noir), changer le titre de l'article 9a : « ~~Protection des données personnelles~~ **Données des personnes morales** » ;

- No 112 (ordonnance sur le service civil), article 110 al. 1 « Le CIVI **est** une banque de données… » ;

- No 116 (OAMal), art. 59a al. 1 in fine : « Le DFI fixe **au niveau suisse** la structure uniforme des ensembles de données » ;

- Art. 59a al. 7 in fine : « Il publie une liste des services **certifiés** de réception des données. ».

* * *