Association Suisse des Délégués
à la Protection des Données (ASDPO)
asdpo.swiss
contact@asdpo.swiss

Genève, le 14 octobre 2021

Département fédéral
de justice et police
A l'att. de Monsieur
Jonas Amstutz
jonas.amstutz@bj.admin.ch

Réponse de l'ASDPO à la consultation sur l'avant-projet d'ordonnance relative à la loi fédérale sur la protection des données (OLPD)

Monsieur,

Pour donner suite à l'ouverture le 23 juin 2021 de la consultation concernant la révision de l'ordonnance sur la protection des données, l'Association Suisse des Délégués à la Protection des Données (ASDPO) a l'honneur de vous faire parvenir ci-dessous sa prise de position sur l'avant-projet mentionné en objet.

Conformément à ses statuts, l'ASDPO poursuit notamment les buts suivants qui légitiment sa participation à ladite consultation :

- promouvoir et développer la fonction de délégués (ou conseillers) à la protection des données en Suisse ;
- participer à des consultations relatives à l'évolution de la législation sur la protection des données.

Nous restons à votre disposition pour toute question que vous pourriez avoir et vous invitons à vous adresser directement comité de l'association au moyen de l'adresse e-mail susmentionnée.

En vous remerciant de l'attention que vous porterez à ce document, nous vous prions d'agréer, Monsieur, l'expression de notre considération distinguée.

François Charlet
Président

Nesrin Keles & Isabelle Hering
Membres du comité

Annexe : prise de position du 13 octobre 2021 de l'ASDPO sur l'avant-projet d'OLPD

Prise de position du 13 octobre 2021 de l'ASDPO sur l'avant-projet d'OLPD

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
Art. 1 Principes [1] Pour savoir si les mesures techniques ou organisationnelles visant à garantir la sécurité des données sont adaptées au risque, les critères suivants sont pris en considération : a. la finalité, la nature, l'étendue et les circonstances du traitement des données ; b. la probabilité d'une violation de la sécurité des données et son impact potentiel sur les personnes concernées ; c. l'état de la technique ; d. les coûts de mise en œuvre. [2] Les mesures sont réexaminées à des intervalles appropriés pendant toute la durée du traitement.	Ces principes sont bienvenus. Cependant, au vu de l'art. 8 al. 3 nLPD, on s'attendait à ce que le Conseil fédéral édicte un catalogue de mesures minimales de sécurité, et non une liste de critères à considérer pour que les entités soumises à la nLPD décident des mesures de sécurité à appliquer. En outre, la violation de ces exigences minimales de sécurité est punissable pénalement selon l'art. 61 let. c nLPD. Le fait de ne pas détailler précisément quelles sont ces exigences pose un réel problème en regard de l'art. 1 CP. Il n'est pas clair quand la responsabilité pénale sera engagée.	Fournir une réelle liste de mesures minimales de sécurité, qui peuvent être sélectionnées dans la liste de l'art. 2.
Art. 2 Objectifs de protection Dans la mesure du possible, les mesures de sécurité des données doivent permettre d'atteindre les objectifs de protection suivants : a. contrôle de l'accès aux données : l'accès des personnes autorisées est limité aux données personnelles dont elles ont besoin pour accomplir leurs tâches ; b. contrôle de l'accès aux locaux et installations : l'accès aux locaux et aux installations utilisées pour le traitement de données personnelles est refusé aux personnes non autorisées ; c. contrôle des supports de données : les personnes non autorisées ne peuvent pas lire, copier, modifier, déplacer ou supprimer des supports de données ; d. contrôle de mémoire : les personnes non autorisées ne peuvent ni introduire de données personnelles dans la mémoire ni consulter, modifier ou effacer des données personnelles enregistrées ;	Lettre d : contrôle de mémoire, le terme « mémoire » ne paraît pas en adéquation avec la description de l'objectif de protection. Des mesures de sécurité des données doivent permettre d'atteindre les objectifs dans tous les cas et non « dans la mesure du possible » car cela laisse une trop grande marge de manœuvre pour la mise en place de la sécurité des données.	Remplacer « mémoire » par « intégrité » semble plus correct d'un point de vue de sécurité informatique. Modifier la phrase introductive : *« En considérant les principes énoncés à l'art.1, les mesures de sécurité des données doivent permettre d'atteindre les objectifs de protection suivants… »*

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
e. contrôle d'utilisation : les personnes non autorisées ne peuvent pas utiliser les systèmes de traitement automatisé de données personnelles au moyen d'installations de transmission ; f. contrôle du transport : les personnes non autorisées ne peuvent pas lire, copier, modifier ou effacer des données personnelles lors de leur communication ou lors du transport de supports de données ; g. contrôle de la saisie : l'identité des personnes saisissant ou modifiant des données personnelles dans le système automatisé, ainsi que les données saisies ou modifiées et le moment de leur saisie ou modification peuvent être vérifiés ; h. contrôle de la communication : il doit être possible de vérifier à qui sont communiquées des données personnelles à l'aide d'installations de transmission ; i. restauration : la disponibilité des données personnelles et l'accès aux données personnelles peuvent être rapidement rétablis en cas d'incident physique ou technique ; j. toutes les fonctions du système doivent être disponibles (disponibilité), les dysfonctionnements éventuels doivent être signalés (fiabilité) et les données personnelles stockées ne doivent pas pouvoir être endommagées par des dysfonctionnements du système (intégrité des données) ; k. détection : les violations de la sécurité des données doivent pouvoir être rapidement détectées et des mesures doivent pouvoir être prises pour réduire ou éliminer les conséquences.		
Art. 3 Journalisation 1 Lorsque l'analyse d'impact sur la protection des données révèle que, malgré les mesures prévues par le responsable du traitement, le traitement envisagé présente encore un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées, le responsable du traitement privé et son sous-traitant journalisent au moins les opérations suivantes :	Al. 4 : pourquoi un délai de deux ans ? De manière générale, d'où proviennent les délais introduits dans le P-OLPD et ne serait-il pas pertinent de les uniformiser ? P. ex. en adoptant partout un délai de 5 ans identique à celui de la prescription pénale de l'art. 66 nLPD. La différence de traitement entre les responsables du traitement privés et les organes fédéraux n'a pas lieu d'être et ne peut être objectivement justifiée.	Harmoniser tous les délais de conservation à 5 ans. Supprimer la différence entre les responsables du traitement privés et les organes fédéraux.

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
enregistrement, modification, lecture, communication, effacement ou destruction. 2 Lors du traitement automatisé de données personnelles, l'organe fédéral et son sous-traitant journalisent au moins les opérations suivantes : enregistrement, modification, lecture, communication, effacement ou destruction. 3 La journalisation doit 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. 4 Les procès-verbaux de journalisation sont conservés durant deux ans, séparément du système dans lequel les données personnelles sont traitées. Ils sont accessibles aux seuls organes ou personnes chargés de vérifier l'application des dispositions de protection des données personnelles ou de rétablir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, et ils ne sont utilisés qu'à cette fin.		
Art. 4 Règlement de traitement des personnes privées 1 Le responsable du traitement et son sous-traitant établissent un règlement pour les traitements automatisés en cas : a. de traitement de données sensibles à grande échelle, ou b. de profilage à risque élevé. 2 Le règlement de traitement contient au moins des indications sur : a. la finalité du traitement ; b. les catégories de personnes concernées et les catégories de données personnelles traitées ; c. la durée de conservation des données personnelles ou les critères utilisés pour déterminer cette durée ; d. l'organisation interne ; e. l'origine des données personnelles et leur mode de collecte ;	Aucune base légale dans la nLPD ne permet d'édicter cet article.	Supprimer la disposition.

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
f. les mesures techniques et organisationnelles visant à garantir la sécurité des données ; g. les autorisations d'accès, ainsi que sur la nature et l'étendue de cet accès ; h. les mesures prises pour la minimisation des données ; i. les procédures de traitement des données, notamment les procédures, d'enregistrement, de rectification, de communication, de conservation, d'archivage, de pseudonymisation, d'anonymisation et d'effacement ou de destruction des données ; j. la procédure d'exercice du droit d'accès et du droit à la remise ou à la transmission des données personnelles. 3 La personne privée actualise régulièrement le règlement et le met à la disposition du conseiller à la protection des données sous une forme qui lui est intelligible.		
Art. 5 Règlement de traitement des organes fédéraux 1 L'organe fédéral responsable et son sous-traitant établissent un règlement pour les traitements automatisés en cas : a. de traitement de données sensibles ; b. de profilage ; c. de traitement de données personnelles au sens de l'art. 34, al. 2, let. c, LPD ; d. d'accès aux données personnelles accordé à des cantons, des autorités étrangères, des organisations internationales ou des personnes privées ; e. d'ensembles de données interconnectés, ou f. d'exploitation d'un système d'information ou de gestion d'ensembles de données conjointement avec d'autres organes fédéraux. 2 Le règlement de traitement contient au moins les indications prévues à l'art. 4, al. 2. 3 L'organe fédéral responsable actualise régulièrement le règlement et le met à la disposition du conseiller à la	Aucune base légale dans la nLPD ne permet d'édicter cet article.	Supprimer la disposition.

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
protection des données sous une forme qui lui est intelligible, ainsi qu'à la disposition du Préposé fédéral à la protection des données et à la transparence (PFPDT), si celui-ci en fait la demande.		
Art. 6 Modalités 1 Le responsable du traitement qui confie un traitement de données personnelles à un sous-traitant demeure responsable de la protection des données. Il s'assure que les données soient traitées conformément au contrat ou à la loi. 2 Lorsqu'un sous-traitant n'est pas soumis à la LPD, le responsable du traitement s'assure que d'autres dispositions légales garantissent une protection équivalente. A défaut, il s'assure qu'une telle protection est garantie par des clauses contractuelles. 3 Lorsque le responsable de traitement est un organe fédéral, le sous-traitant ne peut sous-traiter le traitement des données à un tiers que si l'organe fédéral l'a approuvé par écrit.	Al. 1 : il est problématique que les données doivent être traitées conformément au contrat ou à la loi. Si le contrat déroge à la loi, le sous-traitant pourrait ne pas respecter la loi. Al. 2 : l'obligation de garantir la sécurité des données figure déjà dans la loi. En outre, des mesures contractuelles seules peuvent ne pas suffire. Enfin, quelles sont les situations dans lesquelles un sous-traitant n'est pas soumis à la nLPD, au vu du champ d'application territorial de cette dernière (art. 3 al. 1 nLPD) ? Al. 3 : la sous-sous-traitance devrait être conditionnée à un accord écrit également pour les responsables du traitement privé.	Al. 1 : supprimer la seconde phrase. Al. 2 : « Lorsqu'un sous-traitant n'est pas soumis à la LPD, le responsable du traitement s'assure que d'autres dispositions légales garantissent une protection équivalente. A défaut, il s'assure qu'une telle protection est garantie par des clauses contractuelles, ainsi que des mesures organisationnelles et techniques. » Al. 3 : « ~~Lorsque le responsable de traitement est un organe fédéral~~, le sous-traitant ne peut sous-traiter le traitement des données à un tiers que si le responsable de traitement l'a approuvé par écrit. »
Art. 7 Information du conseiller à la protection des données de l'organe fédéral L'organe fédéral informe sans délai le conseiller à la protection des données de la conclusion d'un contrat avec un sous-traitant ou de l'autorisation de sous-traiter le traitement des données à un tiers. Il informe également le conseiller à la protection des données si des problèmes surviennent dans le respect des exigences légales ou contractuelles de protection des données personnelles.	/	/
Art. 8 Évaluation du niveau de protection adéquat des données personnelles d'un État étranger ou d'un organisme international	Al. 3 : la fréquence de la réévaluation périodique est manquante. Se calquer sur le RGPD.	Al. 3 : "Le niveau de protection dans l'Etat, le territoire, le ou les secteurs déterminés dans un Etat, ou l'organisme international concerné, est réévalué

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
1 En cas de communication de données personnelles à l'étranger, les critères suivants doivent notamment être pris en compte pour évaluer si un État, un territoire, un ou plusieurs secteurs déterminés dans un Etat, ou si un organisme international garantit un niveau de protection adéquat : a. les engagements internationaux de l'État ou de l'organisme international en matière de protection des données personnelles ; b. le respect des droits humains ; c. la législation applicable en matière de protection des données, de même que sa mise en œuvre et la jurisprudence y relative ; d. la garantie effective des droits des personnes concernées et des voies de droit ; e. le fonctionnement effectif d'une ou de plusieurs autorités indépendantes chargées de la protection des données dans l'État concerné, ou auxquelles un organisme international est soumis, et disposant de pouvoirs et de compétences suffisants. 2 L'évaluation peut tenir compte des appréciations effectuées par des organismes internationaux ou des autorités étrangères chargées de la protection des données personnelles. 3 Le niveau de protection dans l'État, le territoire, le ou les secteurs déterminés dans un État, ou l'organisme international concerné, est réévalué périodiquement. 4 Lorsqu'il est constaté, à l'issue de l'évaluation visée à l'al. 3, ou lorsque les informations disponibles révèlent qu'un État, un territoire, un ou plusieurs secteurs déterminés dans un État, ou un organisme international n'assure plus un niveau de protection adéquat, la décision au sens de l'art. 16, al. 1, LPD est modifiée, suspendue ou abrogée. La nouvelle décision n'a pas d'effet sur la communication des données déjà effectuée. 5 Les États, les territoires, les secteurs déterminés dans un États, et les organismes internationaux avec	Al. 4 : indiquer que la nouvelle décision n'a pas d'effet sur les données déjà transférées à l'étranger est erroné. Le responsable du traitement doit réévaluer la situation lorsqu'une décision d'adéquation est modifiée, suspendue ou abrogée, et généralement sélectionner un autre mécanisme s'il souhaite continuer à transférer des données. Les données déjà transférées l'ont certes été sous un régime d'adéquation, mais elles sont désormais traitées dans un État qui n'offre plus de niveau de protection adéquat, ce qui peut porter atteinte aux droits de la personnalité des personnes concernées. Il n'est pas acceptable de tolérer cette situation. Quelle est la procédure applicable à la prise de décision ? Les États concernés peuvent-ils recourir ?	périodiquement, mais au maximum tous les quatre ans." Al. 4 : supprimer la dernière phrase.

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
un niveau de protection adéquat sont mentionnés à l'annexe 1. 6 Le PFPDT est consulté avant toute décision portant sur l'adéquation.		
Art. 9 Clauses de protection des données d'un contrat et garanties spécifiques 1 Les clauses de protection des données d'un contrat au sens de l'art. 16, al. 2, let. b, LPD et les garanties spécifiques au sens de l'art. 16, al. 2, let. c, LPD portent au moins sur les points suivants : a. l'application des principes de licéité, de bonne foi, de proportionnalité, de finalité et d'exactitude ; b. les catégories de données communiquées et de personnes concernées ; c. le type et la finalité de la communication des données personnelles ; d. le nom des Etats de destination ; e. le nom des organismes internationaux de destination ; f. les conditions applicables à la conservation, l'effacement et la destruction des données personnelles ; g. les destinataires habilités à traiter les données ; h. les mesures garantissant la sécurité des données personnelles ; i. les conditions applicables à la communication des données à un autre Etat étranger ou à un autre organisme international ; j. l'obligation pour les destinataires d'informer les personnes concernées par le traitement des données ; k. les droits de la personne concernée, en particulier : 1. de demander l'accès à ses données personnelles, 2. de s'opposer au traitement des données personnelles, 3. de demander la rectification, l'effacement ou la destruction de données personnelles, 4. de saisir en justice une autorité indépendante. 2 Le responsable du traitement prend les mesures adéquates pour s'assurer que le destinataire respecte	Al. 1 : dans l'énumération, il manque un point sur le droit d'audit de l'exportateur des données vis-à-vis de l'importateur (mesure nécessaire pour être en mesure de contrôler le niveau de protection), ainsi qu'un point sur l'obligation d'annonces des violations de la sécurité des données.	Al. 1 let. a : ajouter le principe de transparence/information (cf. art. 16 et 17 nLPD) Al. 1 let. h : "les mesures techniques et organisationnelles" Al. 1 let. k : ajouter le droit à la remise des données (cf. art. 28 et 29 nLPD) Al. 1 : ajouter une lettre m sur le droit d'audit et une lettre n sur l'annonce des violations de la sécurité des données.

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
les clauses de protection des données d'un contrat ou les garanties spécifiques. 3 Une fois les clauses de protection des données d'un contrat ou les garanties spécifiques annoncées au PFPDT, le devoir d'information du responsable du traitement est réputé également rempli pour toutes les communications : a. qui se fondent sur les mêmes clauses ou garanties, pour autant que les catégories de destinataires, les finalités du traitement et les catégories de données communiquées soient similaires, ou b. qui sont effectuées au sein d'une même personne morale ou société ou entre des entreprises appartenant au même groupe, aussi longtemps que les clauses ou les garanties fournies permettent d'assurer une protection appropriée des données.		
Art. 10 Clauses types de protection des données 1 Lorsqu'il communique des données personnelles à l'étranger au moyen de clauses types de protection des données au sens de l'art. 16, al. 2, let. d, LPD, le responsable du traitement prend les mesures adéquates pour s'assurer que le destinataire les respecte. 2 Le PFPDT publie une liste des clauses types de protection des données qu'il a approuvées, établies ou reconnues.	/	/
Art. 11 Règles d'entreprise contraignantes 1 Les règles d'entreprise contraignantes au sens de l'art. 16, al. 2, let. e, LPD s'appliquent à toutes les entreprises appartenant au même groupe. 2 Elles portent au moins sur les points mentionnés à l'art. 9, al. 1, ainsi que sur les points suivants : a. la structure et les coordonnées du groupe d'entreprises et de chacune de ses entités ; b. les mesures mises en place au sein des groupes d'entreprises pour garantir le contrôle du respect des règles d'entreprise contraignantes.	Al. 1 : Qu'entend-on par « groupe d'entreprises » ? Cette notion n'est pas claire quant à la structure de l'organisation et de quelle manière elle est constituée. Faut-il que les entreprises d'un groupe soient détenues à plus de 50% par les mêmes actionnaires ? Quid des succursales ?	Préciser la notion de "groupe d'entreprises".

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
Art. 12 Codes de conduite et certifications 1 Des données personnelles peuvent être communiquées à l'étranger si un niveau de protection approprié est garanti par un code de conduite ou une certification. 2 Le code de conduite porte au moins sur les points mentionnés à l'art. 9, al. 1 et doit être préalablement approuvé par le PFPDT. 3 Le code de conduite ou la certification doit être assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans l'État tiers d'appliquer les mesures contenues dans ces instruments.	Al. 2 : la nLPD indique (art. 11) que "le PFPDT prend position sur les codes de conduites et publie ses prises de position". L'ordonnance va plus loin en exigeant une approbation.	Al. 2 : supprimer l'approbation du PFPDT.
Art. 13 Modalités du devoir d'informer 1 Le responsable du traitement et le sous-traitant communiquent les informations sur la collecte de données personnelles de manière concise, compréhensible et facilement accessible. 2 Lorsque l'information se fait en combinaison de pictogrammes, ceux-ci doivent être lisibles par machine s'ils sont présents par voie électronique.	Il est normalement de la responsabilité du responsable du traitement d'informer les personnes concernées (l'art. 18 nLPD ne mentionne pas le sous-traitant). La situation pouvant néanmoins se présenter en pratique, nous suggérons l'adaptation de l'al. 1 et un nouvel al. 3. Al. 2 : Dans quels contextes ces pictogrammes seraient-ils utilisés ? Aucune information dans la nLPD à ce sujet. Quels types de pictogrammes peuvent être utilisés ? Doivent-ils être reconnus par le PFPDT ?	Al. 1 : Supprimer "et le sous-traitant" Ajouter al. 3 : "Lorsque le responsable du traitement a sous-traité la collecte des données, la communication des informations échoit au sous-traitant."
Art. 14 Disposition particulière relative au devoir d'informer des organes fédéraux lors de la collecte des données personnelles Si la personne concernée n'est pas tenue de fournir des renseignements, l'organe fédéral qui collecte systématiquement des données personnelles notamment au moyen d'un questionnaire doit l'informer du caractère facultatif de sa réponse.	L'obligation d'informer figure dans la nLPD, pourquoi adopter une disposition spécifique relative aux questionnaires ?	Supprimer la disposition.
Art. 15 Informations lors de la communication des données personnelles Le responsable du traitement et le sous-traitant indiquent au destinataire l'actualité, la fiabilité et	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
l'exhaustivité des données personnelles qu'ils communiquent, dans la mesure où ces informations ne ressortent pas des données elles-mêmes ou des circonstances.		
Art. 16 Informations sur la rectification, l'effacement ou la destruction, ainsi que sur la limitation du traitement des données personnelles 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, sauf si la notification est impossible ou implique des efforts disproportionnés.	Les situations dans lesquelles la notification est impossible ne sont pas claires et, en outre, ne devraient jamais se produire. En outre, avec l'informatique, le cloud, les API, etc. cette notification ne devrait pas (ou très rarement) générer des efforts disproportionnés. Cette obligation nécessite de prendre des dispositions particulières en matière d'organisation et de gouvernance, un second alinéa serait pertinent à cet égard.	Supprimer "sauf si la notification est impossible ou implique des efforts disproportionnés". Ajouter un al. 2 : "Le responsable du traitement prend les mesures adéquates, notamment contractuelles et techniques, pour être en mesure de notifier les destinataires auxquels il a communiqué des données personnelles."
Art. 17 Réexamen d'une décision individuelle automatisée La personne concernée par une décision individuelle automatisée, qui demande à faire valoir son point de vue ou un réexamen de la décision par une personne physique, ne peut pas être désavantagée pour ce motif.	/	/
Art. 18 Forme et conservation de l'analyse d'impact relative à la protection des données personnelles Le responsable du traitement consigne par écrit l'analyse d'impact relative à la protection des données personnelles. Elle est conservée pendant deux ans après la fin du traitement des données.	Sur quelle base ce délai de deux ans a été défini ? De manière générale, quelles raisons ont mené à adopter des délais différents entre les articles 18 et 19 P-OLPD ? En outre, la conservation sous la forme écrite n'est pas souhaitable en regard des art. 12 et suivants CO.	Harmoniser tous les délais de conservation à 5 ans. Remplacer "par écrit" par "par tout moyen qui permet d'en apporter la preuve".
Art. 19 Annonce des violations de la sécurité des données 1 En cas de violation de la sécurité des données, le responsable du traitement annonce au PFPDT : a. la nature de la violation ; b. dans la mesure du possible, le moment et la durée ;	Al. 1 : le responsable du traitement doit être contraint dans tous les cas de fournir les informations des let. b, c et d. Il n'est pas acceptable que ces informations puissent être fournies que "dans la mesure du possible". Ces informations seront disponibles tôt ou tard dans tous les cas.	Al. 1 : Supprimer « dans la mesure du possible » aux let. b, c et d. Al. 2 : "Si le responsable du traitement n'est pas en mesure de fournir au PFPDT toutes les informations visées à l'al. 1 dans les meilleurs délais..."

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
c. dans la mesure du possible, les catégories et le nombre approximatif de données personnelles concernées ; d. dans la mesure du possible, les catégories et le nombre approximatif de per- sonnes concernées ; e. les conséquences, y compris les risques éventuels, pour les personnes concernées ; f. les mesures prises ou envisagées pour remédier à cette défaillance ou en atténuer les conséquences ; g. le nom et les coordonnées d'une personne de contact. 2 Si, lors de la détection de la violation de la sécurité des données, le responsable du traitement n'est pas en mesure de fournir au PFPDT toutes les informations visées à l'al. 1 dans le même temps, il peut les lui mettre à disposition progressivement sans retard excessif. 3 Le responsable du traitement communique à la personne concernée, dans un langage simple et compréhensible, au moins les informations visées à l'al. 1, let. a, e, f et g. 4 Lorsque le responsable du traitement est un organe fédéral, l'annonce au PFPDT est faite par l'intermédiaire du conseiller à la protection des données personnelles. 5 Le responsable du traitement documente les violations. La documentation contient tous les faits relatifs aux incidents, à leurs effets et aux mesures prises. Elle est conservée pendant au moins trois ans à compter de la date d'annonce, au sens de l'al. 1.	Al. 2 : Selon l'art. 24 al. 1 nLPD, il est indiqué que le responsable du traitement annonce dans les meilleurs délais au PFDT les violations de sécurité de données, et non lors de la détection de la violation. Al. 3 : les let. b et c devraient également être incluses, car ces informations peuvent aider les personnes concernées à déterminer l'étendue de l'incident et prendre les mesures qui s'imposent. Al. 5 : Peu clair. Quelles violations doivent être documentées ? Celles annoncées ou celles non annoncées ? Les deux ? Bien qu'il existe des doutes quant à la légalité de cet alinéa, il est utile que toutes les violations soient documentées, 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. Renvoi à la réflexion de l'article 18 P-OLPD pour le délai de trois ans.	Al. 5 : Le responsable du traitement documente toutes les violations. Harmoniser tous les délais de conservation à 5 ans.
Art. 20 Modalités 1 La demande de renseignement est faite par écrit. Elle peut être faite oralement moyennant l'accord du responsable du traitement. 2 Les renseignements sont en principe fournis par écrit. D'entente avec le responsable du traitement, ou sur sa proposition, la personne concernée peut également consulter ses données sur place. Si elle y a consenti,	Al. 2 : « par écrit » → même remarque que pour l'art. 18. Ici, la forme écrite ne devrait pas être érigée en principe, le responsable du traitement devrait être libre de proposer différents modes de transmission (en particulier électronique) pour autant qu'ils soient sécurisés et fiables. En outre, la personne concernée devrait pouvoir proposer de consulter les données sur	Al. 2 : supprimer la forme écrite ou y ajouter la forme électronique. Supprimer « ou sur sa proposition ». Al. 5 : "Le responsable du traitement documente le motif pour lequel il refuse, restreint ou diffère la communication des informations. La documentation est conservée pendant au moins cinq ans."

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
les renseignements peuvent également lui être fournis oralement. 3 Les renseignements fournis doivent être compréhensibles pour la personne concernée. 4 Le responsable du traitement prend les mesures adéquates pour assurer l'identification de la personne concernée et pour protéger les données de la personne concernée de tout accès de tiers non autorisé lors de la communication des renseignements. La personne concernée est tenue de collaborer à son identification. 5 Le responsable du traitement documente le motif pour lequel il refuse, restreint ou diffère la communication des informations. La documentation est conservée pendant au moins trois ans.	place, cette prérogative ne devrait pas appartenir uniquement au responsable du traitement. Al. 5 : La durée de 3 ans est trop courte. Prévoir au moins 5 ans (cf. supra). La terminologie utilisée (informations, renseignements) prête à confusion. Parle-t-on des mêmes données ? Il serait opportun d'uniformiser la terminologie.	Uniformiser la terminologie.
Art. 21 Responsabilité 1 Lorsqu'il existe plusieurs responsables pour le traitement des données personnelles, la personne concernée peut exercer son droit d'accès auprès de chacun d'eux. Si l'un des responsables du traitement n'est pas compétent pour traiter la demande, il la transmet au responsable du traitement compétent. 2 Si la demande de renseignement porte sur des données traitées par un sous-traitant, le responsable du traitement transmet la demande au sous-traitant s'il n'est pas en mesure de fournir les renseignements lui-même.	Il est regrettable 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 : "il la transmet sans délai..."
Art. 22 Délais 1 Les renseignements sont fournis dans les 30 jours suivant réception de la demande. Si le responsable du traitement refuse, restreint ou diffère le droit d'accès, il le communique dans le même délai. 2 Si les renseignements ne peuvent être donnés dans les 30 jours, le responsable du traitement en avertit la personne concernée en lui indiquant le délai dans lequel les renseignements seront fournis.	Al. 2 : selon l'art. 25 al. 7 nLPD, en règle générale, les renseignements sont fournis dans un délai de 30 jours (suivant réception de la requête). Il doit en être de même pour toutes les situations qu'il s'agisse d'une demande de renseignements ou d'un refus d'accès.	Al. 2 : "Si les renseignements, ou si la décision relative au refus, à la restriction ou au report du droit d'accès, ne peuvent être donnés dans les 30 jours, le responsable du traitement en avertit la personne concernée en lui indiquant le délai dans lequel ceux-ci seront fournis."

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
Art. 23 Exceptions à la gratuité 1 Une participation équitable aux frais peut être demandée lorsque la communication des renseignements occasionne des efforts disproportionnés. 2 Le montant prélevé s'élève à 300 francs au maximum. 3 La personne concernée est préalablement informée du montant et peut retirer sa requête dans les dix jours.	Al. 3 : Est-ce que ce délai de 10 jours suspend le délai global de 30 jours de l'art. 25 al. 7 nLPD et de l'art. 22 P-OLPD ? En effet, le responsable du traitement peut mettre quelques jours à déterminer si la requête sort du principe de la gratuité et, ce faisant, « travaille » déjà à y répondre. Bien qu'il soit contraire au principe du droit d'accès d'exiger le paiement de frais, il serait bienvenu (pour la sécurité du droit et la pratique) d'indiquer qu'en l'absence de réponse, et après un rappel, la personne concernée est réputée avoir retiré sa requête.	Al. 3 : "La personne concernée est préalablement informée du montant et peut retirer sa requête dans les dix jours. La requête est réputée retirée dans le cas où, après un rappel, le montant demandé n'est pas payé dans le second délai de 10 jours." Préciser aussi si le délai de 10 jours suspend le délai de 30 jours.
Art. 24 Les art. 20 al. 1, 4 et 5, ainsi que 21, 22 et 23 s'appliquent par analogie à la remise et à la transmission des données personnelles, ainsi qu'à leurs éventuelles restrictions.	/	/
Art. 25 Conseiller à la protection des données 1 Le conseiller à la protection des données personnelles d'un responsable du traitement privé doit accomplir les tâches suivantes : a. contrôler le traitement de données personnelles ainsi que ses exigences et proposer des mesures s'il constate que des prescriptions de protection des données ont été violées ; b. concourir à l'établissement de l'analyse d'impact relative à la protection des données, et la vérifier, dans tous les cas lorsque le responsable du traitement privé entend renoncer à consulter le PFPDT au sens de l'art. 23, al. 4, LPD ; 2 Le responsable du traitement privé : a. met à disposition du conseiller à la protection des données personnelles les ressources nécessaires ; b. donne au conseiller à la protection des données accès à tous les renseignements, documents, registres des activités de traitement et données personnelles dont il a besoin pour l'accomplissement de ses tâches.	Ces précisions sont bienvenues, mais la nLPD laisse-t-elle la possibilité au Conseil fédéral de compléter ainsi la loi sur des aspects impliquant les personnes privées ? L'art. 10 al. 4 nLPD ne mentionne que les organes fédéraux. La base légale semble (malheureusement) manquante.	A regret : supprimer l'art. 25. Si la disposition est maintenue : • Décrire plus précisément les tâches du conseiller (p. ex. sous la forme d'un inventaire ou d'une description de fonction) • Rapprocher le plus possible la fonction de conseiller d'un responsable du traitement privé de la fonction de conseiller d'un organe fédéral (cf. art. 29) • Préciser quelle est la responsabilité (civile, pénale) du conseiller

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
Art. 26 Exception à l'obligation de tenir un registre des activités de traitement Les entreprises et autres organismes de droit privé employant moins de 250 collaborateurs au début d'une année, ainsi que les personnes physiques, sont déliés de leur obligation de tenir un registre des activités de traitement, à moins que l'une des conditions suivantes soit remplie : a. le traitement porte sur des données sensibles à grande échelle ; b. le traitement constitue un profilage à risque élevé.	C'est cohérent avec l'art. 22 al. 2 nLPD mais problématique. Le simple fait de traiter des données sensibles, de réaliser des profilages, d'utiliser des techniques de machine learning et de traiter de grandes quantités de données (même non sensibles) etc. est susceptible de créer un risque important pour les personnes concernées. Les exceptions listées sous lettres a et b sont trop larges et s'appliqueront à un grand nombre d'entreprises, ce qui vide de son sens et de son utilité la tenue d'un registre de traitement. La création et la tenue d'un registre, même sous une forme simple pour une PME, sont un exercice indispensable à une bonne gouvernance de la protection et de la sécurité des données. Pousser les entreprises à documenter leurs traitements et les mesures de sécurité associées va dans le sens d'une meilleure responsabilisation des entreprises et protection des personnes concernées. Le rapport explicatif de l'OLPD ne s'y trompe pas puisqu'il affirme que le registre des traitements est un instrument simple et efficace. En outre, le registre des activités de traitement constitue la base pour un programme de protection des données et la prise de mesures de sécurité adéquates.	Prévoir des conditions plus nombreuses, mais moins larges. S'inspirer de l'art. 30 al. 5 RGPD. Le traitement de données sensibles devrait systématiquement conduire à l'établissement d'un registre des traitements, de même que tout traitement constituant un profilage.
Art. 27 Désignation Tout organe fédéral désigne un conseiller à la protection des données personnelles. Plusieurs organes fédéraux peuvent désigner conjointement un conseiller.	/	/
Art. 28 Exigences et tâches 1 Le conseiller à la protection des données personnelles doit remplir les conditions suivantes : a. il dispose des connaissances professionnelles nécessaires ;	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
b. il exerce sa fonction de manière indépendante par rapport à l'organe fédéral et sans recevoir d'instruction de celui-ci. 2 Il accomplit les tâches suivantes : a. contrôler le traitement de données personnelles ainsi que ses exigences et proposer des mesures s'il constate que des prescriptions de protection des données ont été violées ; b. concourir à l'établissement de l'analyse d'impact relative à la protection des données et la vérifier ; c. annoncer au PFPDT les violations de la sécurité des données ; d. servir de point de contact pour les personnes concernées ; f. former et conseiller l'organe fédéral et ses collaborateurs en matière de protection des données.		
Art. 29 Devoirs de l'organe fédéral 1 L'organe fédéral donne au conseiller à la protection des données accès à tous les renseignements, documents, registres des activités de traitement et données personnelles dont il a besoin pour l'accomplissement de ses tâches. 2 Il publie les coordonnées du conseiller à la protection des données personnelles en ligne et les communique au PFPDT.	/	/
Art. 30 Interlocuteur du PFPDT Le conseiller à la protection des données personnelles est l'interlocuteur du PFPDT fédéral pour les questions relatives au traitement des données personnelles par l'organe concerné.	/	/
Art. 31 Information du conseiller à la protection des données L'organe fédéral responsable informe le conseiller à la protection des données en temps utile lors de la conception d'un projet de traitement automatisé de données personnelles, ainsi qu'en cas de modifications après l'achèvement du projet, afin que les exigences de	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
la protection des données soient prises en compte à temps.		
Art. 32 Annonce au PFPDT 1 L'organe fédéral responsable informe le PFPDT des activités prévues de traitement automatisé au moment de l'approbation du projet ou de la décision de le développer. Le PFPDT enregistre cette information dans le registre des activités de traitement. 2 L'annonce contient les informations prévues à l'art. 12, al. 2, let. a à d LPD, ainsi que la date prévue pour le début des activités de traitement. 3 L'organe fédéral responsable actualise cette annonce lors du passage à la phase de production ou lorsque le projet est abandonné.	/	/
Art. 33 Caractère indispensable de la phase d'essai Une phase d'essai, en tant qu'essai pilote, peut être considérée comme indispensable si l'une des conditions suivantes est remplie : a. l'accomplissement des tâches nécessite l'introduction d'innovations techniques dont les effets doivent être évalués ; b. l'accomplissement des tâches nécessite la prise de mesures organisationnelles ou techniques importantes dont l'efficacité doit être examinée, notamment dans le cadre d'une collaboration entre les organes fédéraux et les cantons ; c. l'accomplissement des tâches nécessite de rendre accessibles en ligne les données personnelles faisant l'objet d'un traitement.	/	/
Art. 34 Autorisation 1 Avant de consulter les unités administratives concernées, l'organe fédéral responsable de l'essai pilote communique au PFPDT de quelle manière il est prévu d'assurer que les exigences de l'art. 35 LPD sont remplies et l'invite à prendre position. 2 Le PFPDT prend position sur le respect des exigences de l'art. 35 LPD. A cet effet, l'organe fédéral	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
responsable lui remet tous les documents nécessaires et en particulier : a. un descriptif général de l'essai pilote ; b. un rapport démontrant que l'accomplissement des tâches légales nécessite le traitement au sens de l'art. 34, al. 2, LPD et rend indispensable une phase d'essai avant l'entrée en vigueur de la loi au sens formel (art. 35, al. 1, let. c, LPD) ; c. un descriptif de l'organisation interne et des processus de traitement et de contrôle des données ; d. un descriptif des mesures de sécurité et de protection des données ; e. un projet d'ordonnance réglant les modalités de traitement ou les grandes lignes de cet acte législatif ; f. les informations concernant la planification des différentes phases de l'essai pilote. 3 Le PFPDT peut exiger d'autres documents et procéder à des vérifications complémentaires. 4 L'organe fédéral responsable informe le PFPDT de toute modification essentielle portant sur le respect des conditions de l'art. 35 LPD. Le cas échéant, le PFPDT prend à nouveau position. 5 La prise de position du PFPDT est annexée à la proposition adressée au Conseil fédéral. 6 Les modalités du traitement automatisé sont réglées par voie d'ordonnance.		
Art. 35 Rapport d'évaluation L'organe fédéral responsable soumet pour avis au PFPDT le projet de rapport portée à la connaissance du Conseil fédéral.	/	/
Art. 36 Lorsque des données personnelles sont traitées à des fins ne se rapportant pas à des personnes, en particulier en cas de recherche, de planification ou de statistique, et que le traitement sert également une autre finalité, les dérogations prévues à rapportant pas à des personnes.	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
Art. 37 Siège et secrétariat permanent 1 Le siège du PFPDT est à Berne. 2 Les rapports de travail du personnel du secrétariat permanent du PFPDT sont régis par la législation fédérale sur le personnel. Le personnel du secrétariat permanent du PFPDT est assuré auprès de la Caisse de pensions PUBLICA, à savoir la Caisse de prévoyance de la Confédération, contre les conséquences économiques de la vieillesse, de l'invalidité et du décès.	/	/
Art. 38 Moyen de communication 1 Le PFPDT communique avec le Conseil fédéral par l'intermédiaire du Chancelier de la Confédération. Celui-ci transmet les propositions, prises de positions et rapports au Conseil fédéral sans les modifier. 2 Le PFPDT transmet les rapports destinés à l'Assemblée fédérale par l'intermédiaire des Services du Parlement.	/	/
Art. 39 Communication des directives et des décisions 1 Les départements et la Chancellerie fédérale communiquent au PFPDT leurs directives en matière de protection des données, ainsi que leurs décisions sous forme anonyme. 2 Les organes fédéraux communiquent au PFPDT tous leurs projets législatifs concernant la protection des données personnelles et l'accès aux documents officiels.	/	/
Art. 40 Traitement des données Le PFPDT traite les données personnelles, y compris les données sensibles, notamment aux fins suivantes : a. exercer ses activités de surveillance ; b. enquêter sur les violations des règles de protection des données ; c. former et conseiller des organes fédéraux et des personnes privées ; d. collaborer avec les autorités cantonales, fédérales et étrangères ;	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
e. mettre en œuvre des procédures de conciliation et des évaluations au sens de la loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration (LTrans) ; f. répondre aux questions des citoyens.		
Art. 41 Autocontrôle 1 Le PFPDT établit un règlement pour tous les traitements automatisés. L'art. 5, al. 1 ne s'applique pas. 2 Il prévoit des processus internes afin de garantir que le traitement des données soit effectué conformément au règlement de traitement. Il vérifie annuellement le respect du règlement de traitement.	/	/
Art. 42 Collaboration avec le Centre national pour la cybersécurité (NCSC) 1 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. Le PFPDT doit au préalable obtenir l'accord de la personne responsable de l'annonce. 2 Il invite le NCSC à se prononcer avant d'ordonner une mesure au sens de l'art. 51, al. 3, let. b, LPD à l'encontre de l'organe fédéral concernant la sécurité des données.	/	/
Art. 43 Registre des activités de traitement des organes fédéraux 1 Le registre des activités de traitement des organes fédéraux contient les informations fournies par les organes fédéraux et leurs sous-traitants conformément à l'art. 12, al. 2 et 3, LPD, ainsi qu'à l'art. 32, al. 2, de la présente ordonnance. 2 Il est publié en ligne. Les inscriptions au registre concernant les activités prévues de traitement automatisé, au sens de l'art. 32, ne sont pas publiées.	/	/
Art. 44 Codes de conduite	/	/

Dispositions du projet d'OLPD	Remarques de l'ASDPO	Propositions d'adaptation
Si un code de conduite est soumis au PFPDT, celui-ci indique dans sa prise de position si le code de conduite remplit les conditions de l'art. 22, al. 5, let. a et b, LPD.		
Art. 45 Emolument 1 L'émolument perçu par le PFPDT se calcule en fonction du temps consacré. 2 Il varie entre 150 et 350 francs l'heure. Il dépend de la complexité de l'affaire et de la fonction de la personne chargée de la traiter. 3 L'ordonnance générale sur les émoluments du 8 septembre 2004s'applique pour le surplus.	/	/
Art. 46 Abrogation et modification d'autres actes L'abrogation est la modification d'autres actes sont réglés à l'annexe 2.	/	/
Art. 47 Disposition transitoire concernant l'annonce au PFPDT des activités prévues de traitement automatisé L'art. 32 ne s'applique pas aux activités prévues de traitement automatisé pour lesquelles l'approbation du projet ou la décision de le développer a déjà été prise au moment de l'entrée en vigueur de la présente ordonnance.	/	/
Art. 48 Entrée en vigueur La présente ordonnance entre en vigueur le ...	/	/

L'ASDPO souhaite remercier vivement Mesdames Laura Menétrey, Nesrin Keles, Isabelle Hering, Anne-Sylvie Aubert, Laura Bares et Mounira Fellag, ainsi que Messieurs Lauris Loat, Stéphane Droxler et François Charlet pour leurs contributions éclairées à cette prise de position.