Ordonnance sur la protection des données (OPDo)

du 31 août 2022 (État le 1er décembre 2025)

Le Conseil fédéral suisse,

vu les art. 8, al. 3, 10, al. 4, 12, al. 5, 16, al. 3, 25, al. 6, 28, al. 3, 33, 59, al. 2 et 3 de la loi fédérale du 25 septembre 2020 sur la protection des données (LPD)[1],

arrête:

Chapitre 1 Dispositions générales

Section 1 Sécurité des données

Art. 1 Principes

1 Pour assurer une sécurité adéquate des données, le responsable du traitement et le sous-traitant établissent le besoin de protection des données personnelles et déterminent les mesures techniques et organisationnelles appropriées à prendre par rapport au risque encouru.

2 Le besoin de protection des données personnelles est évalué en fonction des critères suivants:

a. le type de données traitées;

b. la finalité, la nature, l'étendue et les circonstances du traitement.

3 Le risque pour la personnalité ou les droits fondamentaux de la personne concernée est évalué en fonction des critères suivants:

a. les causes du risque;

b. les principales menaces;

c. les mesures prises ou prévues pour réduire le risque;

d. la probabilité et la gravité d'une violation de la sécurité des données, malgré les mesures prises ou prévues.

4 Lors de la détermination des mesures techniques et organisationnelles, les critères suivants sont de plus pris en compte:

a. l'état des connaissances;

b. les coûts de mise en œuvre.

RO **2022** 568

1 RS **235.1**

5 Le besoin de protection des données personnelles, le risque encouru, ainsi que les mesures techniques et organisationnelles sont réévalués pendant toute la durée du traitement. En cas de besoin, les mesures sont adaptées.

Art. 2 Objectifs

En fonction du besoin de protection, le responsable du traitement et le sous-traitant prennent des mesures techniques et organisationnelles pour que les données traitées:

a. ne soient accessibles qu'aux personnes autorisées (confidentialité);

b. soient disponibles en cas de besoin (disponibilité);

c. ne puissent être modifiées sans droit ou par mégarde (intégrité);

d. soient traitées de manière à être traçables (traçabilité).

Art. 3 Mesures techniques et organisationnelles

1 Pour assurer la confidentialité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que:

a. les personnes autorisées n'aient accès qu'aux données personnelles dont elles ont besoin pour accomplir leurs tâches (contrôle de l'accès aux données);

b. seules les personnes autorisées puissent accéder aux locaux et aux installations utilisés pour le traitement de données (contrôle de l'accès aux locaux et aux installations);

c. les personnes non autorisées ne puissent pas utiliser les systèmes de traitement automatisé de données personnelles à l'aide d'installations de transmission (contrôle d'utilisation).

2 Pour assurer la disponibilité et l'intégrité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que:

a. les personnes non autorisées ne puissent pas lire, copier, modifier, déplacer, effacer ou détruire des supports de données (contrôle des supports de données);

b. les personnes non autorisées ne puissent pas enregistrer, lire, modifier, effacer ou détruire des données personnelles dans la mémoire (contrôle de la mémoire);

c. les personnes non autorisées ne puissent pas lire, copier, modifier, effacer ou détruire des données personnelles lors de leur communication ou lors du transport de supports de données (contrôle du transport);

d. la disponibilité des données personnelles et l'accès à celles-ci puissent être rapidement restaurés en cas d'incident physique ou technique (restauration);

e. toutes les fonctions du système de traitement automatisé de données personnelles soient disponibles (disponibilité), que les dysfonctionnements soient signalés (fiabilité) et que les données personnelles stockées ne puissent pas être endommagées en cas de dysfonctionnements du système (intégrité des données);

f. les systèmes d'exploitation et les logiciels d'application soient toujours maintenus à jour en matière de sécurité et que les failles critiques connues soient corrigées (sécurité du système).

3 Pour assurer la traçabilité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que:

a. il soit possible de vérifier quelles données personnelles sont saisies ou modifiées dans le système de traitement automatisé de données, par quelle personne et à quel moment (contrôle de la saisie);

b. il soit possible de vérifier à qui sont communiquées les données personnelles à l'aide d'installations de transmission (contrôle de la communication);

c. les violations de la sécurité des données puissent être rapidement détectées (détection) et que des mesures puissent être prises pour atténuer ou éliminer les conséquences (réparation).

Art. 4 Journalisation

1 Lors de traitements automatisés de données sensibles à grande échelle ou de profilages à risque élevé et lorsque les mesures préventives ne suffisent pas à garantir la protection des données, le responsable du traitement privé et son sous-traitant privé journalisent au moins l'enregistrement, la modification, la communication, l'effacement et la destruction des données ainsi que l'accès aux données. La journalisation est notamment nécessaire lorsque, sans cette mesure, il n'est pas possible de vérifier a posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées.[2]

2 Lors de traitements automatisés de données sensibles, de profilages et de traitements automatisés de données soumis à la directive (UE) 2016/680[3], l'organe fédéral responsable et son sous-traitant journalisent au moins l'enregistrement, la modification, la communication, l'effacement et la destruction des données ainsi que l'accès aux données. Lors d'autres traitements automatisés de données, ils évaluent au préalable le risque pour les droits fondamentaux des personnes concernées. Ils déterminent sur cette base, ainsi qu'en tenant compte de l'état des connaissances et des coûts de mise en œuvre, si et dans quelle mesure les opérations précitées doivent être journalisées. Pour l'évaluation du risque, ils tiennent notamment compte du type de données traitées, ainsi que de la finalité, de la nature, de l'étendue et des circonstances du traitement.[4]

2 Nouvelle teneur selon le ch. I de l'O du 29 oct. 2025, en vigueur depuis le 1er déc. 2025 (RO **2025** 694).

3 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, version du JO L 119 du 4.5.2016, p. 89.

4 Nouvelle teneur selon le ch. I de l'O du 29 oct. 2025, en vigueur depuis le 1er déc. 2025 (RO **2025** 694).

2bis L'examen de la journalisation au sens de l'al. 2 est consigné par écrit. Le résultat et le contenu de l'examen sont communiqués, sur demande, au Préposé fédéral à la protection des données et à la transparence (PFPDT).[5]

3 Pour les données personnelles accessibles à tout un chacun, l'enregistrement, la modification, l'effacement et la destruction des données doivent au moins être journalisés dans les cas prévus aux al. 1 et 2, 1re phrase.[6]

4 La journalisation doit fournir des informations sur l'identité de la personne qui a effectué le traitement, la nature, la date et l'heure du traitement et, cas échéant, l'identité du destinataire des données.

5 Les procès-verbaux de journalisation sont conservés durant au moins un an, séparément du système dans lequel les données personnelles sont traitées. Ils sont accessibles uniquement aux organes et aux personnes chargés de vérifier l'application des dispositions relatives à la protection des données personnelles ou de préserver ou restaurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, et ne peuvent être utilisés qu'à cette fin.

Art. 5 Règlement de traitement des personnes privées

1 Le responsable du traitement privé et son sous-traitant privé 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 comprend en particulier des informations sur l'organisation interne, sur les procédures de traitement et de contrôle des données, ainsi que sur les mesures visant à garantir la sécurité des données.

3 Le responsable du traitement privé et son sous-traitant privé actualisent régulièrement le règlement. S'ils ont nommé un conseiller à la protection des données, ils mettent le règlement à sa disposition.

Art. 6 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 aux cantons, aux autorités étrangères, aux organisations internationales ou aux personnes privées;

e. d'ensembles de données interconnectés, ou

5 Introduit par le ch. I de l'O du 29 oct. 2025, en vigueur depuis le 1er déc. 2025 (RO **2025** 694).

6 Nouvelle teneur selon le ch. I de l'O du 29 oct. 2025, en vigueur depuis le 1er déc. 2025 (RO **2025** 694).

f. d'exploitation d'un système d'information ou de gestion d'ensembles de données conjointement avec d'autres organes fédéraux.

2 Le règlement comprend en particulier des informations sur l'organisation interne, sur les procédures de traitement et de contrôle des données, ainsi que sur les mesures visant à garantir la sécurité des données.

3 L'organe fédéral responsable et son sous-traitant actualisent régulièrement le règlement et le mettent à la disposition du conseiller à la protection des données.

Section 2 Sous-traitance

Art. 7

1 L'autorisation préalable du responsable du traitement permettant au sous-traitant de confier le traitement des données à un tiers peut être de nature spécifique ou générale.

2 En cas d'autorisation générale, le sous-traitant informe le responsable du traitement lorsqu'il envisage de recourir à d'autres tiers ou de les remplacer. Le responsable du traitement peut s'opposer à cette modification.

Section 3 Communication de données personnelles à l'étranger

Art. 8 Évaluation du niveau de protection adéquat des données d'un État, d'un territoire, d'un secteur déterminé dans un État, ou d'un organisme international

1 Les États, les territoires, les secteurs déterminés dans un État, et les organismes internationaux avec un niveau de protection adéquat sont mentionnés à l'annexe 1.

2 Pour évaluer si un État, un territoire, un secteur déterminé dans un État, ou un organisme international garantit un niveau de protection adéquat, les critères suivants sont en particulier pris en compte:

a. les engagements internationaux de l'État ou de l'organisme international, notamment en matière de protection des données;

b. l'état de droit et le respect des droits de l'homme;

c. la législation applicable, notamment 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.

3 Le PFPDT est consulté lors de chaque évaluation. Les appréciations effectuées par des organismes internationaux ou des autorités étrangères chargées de la protection des données peuvent être prises en compte.[7]

4 L'adéquation du niveau de protection est réévaluée périodiquement.

5 Les évaluations doivent être publiées.

6 Lorsque l'évaluation visée à l'al. 4 ou que d'autres informations indiquent que le niveau de protection adéquat n'est plus garanti, l'annexe 1 est modifiée sans effet sur les communications de données déjà effectuées.

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 comprennent au moins les points suivants:

a. l'application des principes de licéité, de bonne foi, de proportionnalité, de transparence, 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 cas échéant, le nom des États ou des organismes internationaux auxquels sont destinées les données personnelles, et les conditions applicables à la communication;

e. les conditions applicables à la conservation, à l'effacement et à la destruction des données personnelles;

f. les destinataires ou les catégories de destinataires;

g. les mesures visant à garantir la sécurité des données;

h. l'obligation d'annoncer les violations de la sécurité des données;

i. l'obligation pour le destinataire, lorsqu'il est responsable du traitement, d'informer les personnes concernées par le traitement des données;

j. les droits de la personne concernée, en particulier:
   1. le droit d'accès et le droit à la remise ou à la transmission des données personnelles,
   2. le droit de s'opposer à la communication des données,
   3. le droit de demander la rectification, l'effacement ou la destruction des données,
   4. le droit de saisir en justice une autorité indépendante.

7 Nouvelle teneur selon le ch. I de l'O du 29 oct. 2025, en vigueur depuis le 1er déc. 2025 (RO **2025** 694).

2 Le responsable du traitement ou, dans le cas de clauses de protection des données d'un contrat, le sous-traitant prend les mesures adéquates pour s'assurer que le destinataire respecte ces clauses 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.

Art. 10 Clauses types de protection des données

1 Lorsque le responsable du traitement ou le sous-traitant 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, il 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. Il communique le résultat de l'examen sur les clauses types qui lui sont soumises dans un délai de 90 jours.

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 respect des règles d'entreprise contraignantes.

3 Le PFPDT communique le résultat de l'examen sur les règles d'entreprise contraignantes qui lui sont soumises dans un délai de 90 jours.

Art. 12 Codes de conduite et certifications

1 Des données personnelles peuvent être communiquées à l'étranger à condition qu'un code de conduite ou qu'une certification garantisse un niveau de protection approprié.

2 Le code de conduite est préalablement soumis au PFPDT pour approbation.

3 Le code de conduite ou la certification doit être assorti d'un engagement contraignant et exécutoire par lequel le responsable du traitement ou le sous-traitant dans l'État tiers garantit qu'il applique les mesures contenues dans ces instruments.

Chapitre 2 Obligations du responsable du traitement

Art. 13 Modalités du devoir d'informer

Le responsable du traitement communique aux personnes concernées les informations sur la collecte de données personnelles de manière concise, transparente, compréhensible et facilement accessible.

Art. 14 Conservation de l'analyse d'impact relative à la protection des données personnelles

Le responsable du traitement conserve l'analyse d'impact relative à la protection des données personnelles pendant au moins deux ans après la fin du traitement des données.

Art. 15 Annonce des violations de la sécurité des données

1 L'annonce au PFPDT d'une violation de la sécurité des données comprend les informations suivantes:

a. la nature de la violation;

b. dans la mesure du possible, le moment et la durée;

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 personnes concernées;

e. les conséquences, y compris les risques éventuels, pour les personnes concernées;

f. les mesures prises ou prévues pour remédier à cette défaillance et atténuer les conséquences, y compris les risques éventuels;

g. le nom et les coordonnées d'une personne de contact.

2 Si le responsable du traitement n'est pas en mesure d'annoncer simultanément toutes les informations, il fournit les informations manquantes dans les meilleurs délais.

3 Si le responsable du traitement est tenu d'informer la personne concernée, il lui communique, dans un langage simple et compréhensible, au moins les informations visées à l'al. 1, let. a et e à g.

4 Le responsable du traitement documente les violations. La documentation contient les faits relatifs aux incidents, à leurs effets et aux mesures prises. Elle est conservée pendant au moins deux ans à compter de la date d'annonce au sens de l'al. 1.

Chapitre 3 Droits de la personne concernée
Section 1 Droit d'accès

Art. 16 Modalités

[1] Toute personne qui demande au responsable du traitement si des données personnelles la concernant sont traitées doit le faire par écrit. La demande peut être faite oralement moyennant l'accord du responsable du traitement.

[2] Les renseignements sont communiqués par écrit ou sous la forme dans laquelle les données se présentent. D'entente avec le responsable du traitement, la personne concernée peut consulter ses données sur place. Si elle y consent, les renseignements peuvent lui être fournis oralement.

[3] La demande de renseignement et la communication des renseignements peuvent être effectuées par voie électronique.

[4] Les renseignements sont communiqués sous une forme compréhensible pour la personne concernée.

[5] Le responsable du traitement prend des mesures adéquates pour identifier la personne concernée. Celle-ci est tenue de coopérer.

Art. 17 Responsabilité

[1] Lorsque plusieurs responsables traitent en commun des données personnelles, la personne concernée peut exercer son droit d'accès auprès de chacun d'eux.

[2] Si la demande de renseignement porte sur des données traitées par un sous-traitant, celui-ci aide le responsable du traitement à fournir les renseignements pour autant qu'il ne réponde pas lui-même à la demande pour le compte du responsable du traitement.

Art. 18 Délais

[1] Les renseignements sont fournis dans les 30 jours suivant la réception de la demande.

[2] Si les renseignements ne peuvent être donnés dans les 30 jours, le responsable du traitement en informe la personne concernée en lui indiquant le délai dans lequel les renseignements seront fournis.

[3] Si le responsable du traitement refuse, restreint ou diffère le droit d'accès, il le communique dans le même délai.

Art. 19 Exception à la gratuité

[1] Si la communication des renseignements occasionne des efforts disproportionnés, le responsable du traitement peut exiger que la personne concernée participe aux coûts de manière adéquate.

[2] Le montant de la participation s'élève à 300 francs au maximum.

3 Le responsable du traitement informe la personne concernée du montant avant de lui communiquer les renseignements. Si la personne concernée ne confirme pas sa demande dans les 10 jours, celle-ci est considérée comme retirée sans occasionner de frais. Le délai prévu à l'art. 18, al. 1, commence à courir à l'expiration du délai de réflexion de 10 jours.

Section 2
Droit à la remise ou à la transmission des données personnelles

Art. 20 Étendue du droit

1 Sont considérées comme des données personnelles que la personne concernée a communiquées au responsable du traitement:

a. les données qu'elle a mises à sa disposition délibérément et en connaissance de cause;

b. les données que le responsable du traitement a collectées au sujet de la personne concernée et qui concernent son comportement dans le cadre de l'utilisation d'un service ou d'un appareil.

2 Ne sont pas considérées comme des données personnelles que la personne concernée a communiquées au responsable du traitement, les données personnelles que celui-ci a générées en évaluant les données personnelles mises à disposition ou observées.

Art. 21 Exigences techniques de mise en œuvre

1 Les formats électroniques couramment utilisés sont les formats qui permettent, moyennant un effort proportionné, de transmettre les données personnelles en vue de leur réutilisation par la personne concernée ou par un autre responsable du traitement.

2 Le droit à la remise ou à la transmission des données personnelles ne crée pas d'obligation pour le responsable du traitement d'adopter ou de conserver des systèmes de traitement de données techniquement compatibles.

3 L'effort est disproportionné lorsque la transmission de données personnelles à un autre responsable du traitement n'est pas possible pour des raisons techniques.

Art. 22 Délais, modalités et responsabilité

Les art. 16, al. 1 et 5, et 17 à 19 s'appliquent par analogie à la remise ou à la transmission des données personnelles.

Chapitre 4
Dispositions particulières pour le traitement de données personnelles par des personnes privées

Art. 23 Conseiller à la protection des données

Le responsable du traitement:

a. met les ressources nécessaires à la disposition du conseiller à la protection des données;

b. donne accès au conseiller à la protection des données à tous les renseignements, les documents, les registres des activités de traitement et à toutes les données personnelles dont il a besoin pour l'accomplissement de ses tâches;

c. donne au conseiller à la protection des données le droit d'informer l'organe supérieur de direction ou d'administration dans les cas importants.

Art. 24 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 1er janvier 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.

Chapitre 5
Dispositions particulières pour le traitement de données personnelles par des organes fédéraux

Section 1 Conseiller à la protection des données

Art. 25 Désignation

Tout organe fédéral désigne un conseiller à la protection des données. Plusieurs organes fédéraux peuvent désigner ensemble un conseiller.

Art. 26 Exigences et tâches

1 Le conseiller à la protection des données remplit les conditions suivantes:

a. il dispose des connaissances professionnelles nécessaires;

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. participer à l'application des dispositions relatives à la protection des données, en particulier:
   1. en contrôlant le traitement de données personnelles et en proposant des mesures correctives lorsqu'une violation des dispositions relatives à la protection des données est constatée,
   2. en conseillant le responsable du traitement lors de l'établissement de l'analyse d'impact relative à la protection des données et en vérifiant son exécution;

b. servir d'interlocuteur pour les personnes concernées;

c. former et conseiller les collaborateurs de l'organe fédéral en matière de protection des données.

Art. 27 Devoirs de l'organe fédéral

1 L'organe fédéral:

a. donne accès au conseiller à la protection des données à tous les renseignements, les documents, les registres des activités de traitement et à toutes les données personnelles dont il a besoin pour l'accomplissement de ses tâches;

b. veille à ce que le conseiller à la protection des données soit informé de toute violation de la sécurité des données.

2 Il publie les coordonnées du conseiller à la protection des données en ligne et les communique au PFPDT.

Art. 28 Interlocuteur du PFPDT

Le conseiller à la protection des données personnelles est l'interlocuteur du PFPDT pour les questions relatives au traitement des données par l'organe fédéral concerné.

Section 2 Devoir d'informer

Art. 29 Devoir d'informer lors de la communication des données personnelles

L'organe fédéral indique au destinataire l'actualité, la fiabilité et l'exhaustivité des données personnelles qu'il communique, dans la mesure où ces informations ne ressortent pas des données elles-mêmes ou des circonstances.

Art. 30 Devoir d'informer lors de la collecte systématique des données personnelles

Si la personne concernée n'est pas tenue de fournir des renseignements, l'organe fédéral qui collecte systématiquement des données personnelles doit l'en informer.

Section 3
Annonce au PFPDT des projets pour le traitement automatisé des données personnelles

Art. 31

[1] L'organe fédéral responsable annonce au PFPDT les activités prévues de traitement automatisé au moment de l'approbation du projet ou de la décision de le développer.

[2] L'annonce contient les indications 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] Le PFPDT enregistre cette annonce dans le registre des activités de traitement.

[4] L'organe fédéral responsable actualise cette annonce lors du passage à la phase de production ou lorsque le projet est abandonné.

Section 4 Essais pilotes

Art. 32 Caractère indispensable de l'essai pilote

Un essai pilote est 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.

Art. 33 Procédure d'autorisation de l'essai pilote

[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 conditions de l'art. 35 LPD soient remplies et l'invite à prendre position.

[2] Le PFPDT prend position sur le respect des conditions de l'art. 35 LPD. À cet effet, l'organe fédéral 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 un traitement selon l'art. 34, al. 2, LPD et rend indispensable une phase d'essai avant l'entrée en vigueur de la loi au sens formel;

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. 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 informe le PFPDT de toute modification essentielle portant sur le respect des conditions de l'art. 35 LPD. Si nécessaire, le PFPDT prend à nouveau position.

5 La prise de position du PFPDT est annexée à la proposition adressée au Conseil fédéral.

6 Le traitement automatisé est réglé par voie d'ordonnance.

Art. 34 Rapport d'évaluation

1 L'organe fédéral responsable soumet le projet de rapport d'évaluation à l'intention du Conseil fédéral au PFPDT pour prise de position.

2 Il soumet le rapport d'évaluation accompagné de la prise de position du PFPDT au Conseil fédéral.

Section 5
Traitement des données à des fins ne se rapportant pas à des personnes

Art. 35

Lorsque des données personnelles sont traitées à des fins ne se rapportant pas à des personnes, en particulier à des fins de recherche, de planification ou de statistique, et que le traitement sert également une autre finalité, les dérogations prévues à l'art. 39, al. 2, LPD ne s'appliquent qu'au seul traitement effectué à des fins ne se rapportant pas à des personnes.

Chapitre 6
Préposé fédéral à la protection des données et à la transparence

Art. 36 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 sur le personnel de la Confédération. Le personnel est assuré auprès de la Caisse de prévoyance de la Confédération.

Art. 37 Voie de communication

[1] Le PFPDT communique avec le Conseil fédéral par l'intermédiaire du chancelier de la Confédération. Celui-ci transmet les propositions, les prises de positions et les 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. 37*a*[8] Conclusion et modification de déclarations d'intention

Le PFPDT rend compte chaque année au Conseil fédéral des déclarations d'intention relatives à la coopération avec des autorités étrangères chargées de la protection des données qu'il a conclues et modifiées.

Art. 38 Communication des décisions, des directives et des projets

[1] En matière de protection des données, les départements et la Chancellerie fédérale communiquent au PFPDT leurs décisions sous forme anonyme, ainsi que leurs directives.

[2] Les organes fédéraux soumettent au PFPDT tous leurs projets législatifs concernant le traitement de données personnelles, la protection des données et l'accès aux documents officiels.

Art. 39 Traitement des données

Le PFPDT peut traiter les données personnelles, y compris les données sensibles, notamment aux fins suivantes:

a. exercer ses activités de surveillance;
b. exercer ses activités de conseil;
c. collaborer avec les autorités cantonales, fédérales et étrangères;
d. exécuter des tâches dans le cadre des dispositions pénales au sens de la LPD;
e. mettre en œuvre des procédures de conciliation et émettre des recommandations au sens de la loi du 17 décembre 2004 sur la transparence (LTrans)[9];
f. mettre en œuvre des évaluations au sens de la LTrans;
g. mettre en œuvre des procédures de demande d'accès au sens de la LTrans;
h. informer la surveillance parlementaire;
i. informer le public;
j. exercer ses activités de formation.

8 Introduit par le ch. I de l'O du 29 oct. 2025, en vigueur depuis le 1er déc. 2025 (RO **2025** 694).
9 RS **152.3**

Art. 40 Autocontrôle

Le PFPDT établit un règlement pour tous les traitements automatisés; l'art. 6, al. 1, ne s'applique pas.

Art. 41[10] Collaboration avec l'Office fédéral de la cybersécurité

1 …[11]

2 Le PFPDT invite l'Office fédéral de la cybersécurité à se prononcer avant d'ordonner à l'organe fédéral de prendre les mesures visées à l'art. 8 LPD.

Art. 42 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 conformément aux art. 12, al. 2, LPD et 31, al. 2, de la présente ordonnance.

2 Il est publié en ligne. Les inscriptions au registre concernant les activités de traitement automatisé prévues, au sens de l'art. 31, ne sont pas publiées.

Art. 43 Codes de conduite

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. 44 Émolument

1 L'émolument perçu par le PFPDT se calcule en fonction du temps consacré.

2 Le tarif horaire varie entre 150 et 250 francs, selon la fonction exercée par la personne concernée.

3 Pour les prestations d'une ampleur extraordinaire, présentant des difficultés particulières ou ayant un caractère urgent, des suppléments pouvant atteindre 50 % de l'émolument prévu à l'al. 2 peuvent être perçus.

4 Si la prestation du PFPDT peut être réutilisée à des fins commerciales par la personne assujettie à l'émolument, des suppléments pouvant atteindre 100 % de l'émolument prévu à l'al. 2 peuvent être perçus.

5 L'ordonnance générale du 8 septembre 2004 sur les émoluments[12] s'applique pour le reste.

10 Nouvelle teneur selon le ch. II 7 de l'O du 22 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 746).
11 Abrogé par l'annexe ch. 2 de l'O du 7 mars 2025 sur la cybersécurité, avec effet au 1er avr. 2025 (RO **2025** 169).
12 RS **172.041.1**

Chapitre 7 Dispositions finales

Art. 45 Abrogation et modification d'autres actes

L'abrogation et la modification d'autres actes sont réglées à l'annexe 2.

Art. 46 Dispositions transitoires

[1] Pour les traitements automatisés de données personnelles planifiés ou ayant débuté avant l'entrée en vigueur de la modification du 29 octobre 2025, l'examen de la journalisation au sens de l'art. 4, al. 2, doit être effectué d'ici au 31 décembre 2026. Si la journalisation s'avère nécessaire, elle doit être mise en œuvre d'ici au 31 décembre 2029. Les traitements automatisés de données sensibles, les profilages et les traitements automatisés de données soumis à la directive (UE) 2016/680[13] ne sont pas visés par la présente disposition.[14]

[2] L'art. 8, al. 5, ne s'applique pas aux évaluations effectuées avant l'entrée en vigueur de la présente ordonnance.

[3] L'art. 31 ne s'applique pas aux activités de traitement automatisé prévues 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. 47 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er septembre 2023.

13 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, version du JO L 119 du 4.5.2016, p. 89.

14 Nouvelle teneur selon le ch. I de l'O du 29 oct. 2025, en vigueur depuis le 1er déc. 2025 (RO **2025** 694).

Annexe 1[15]
(art. 8, al. 1)

États, territoires, secteurs déterminés dans un État et organismes internationaux dans lesquels un niveau de protection adéquat des données est garanti

1	Allemagne*	
2	Andorre***	
3	Argentine***	
4	Autriche*	
5	Belgique*	
6	Bulgarie***	
7	Canada***	Un niveau de protection adéquat est réputé garanti lorsque la loi fédérale canadienne du 13 avril 2000 sur la protection des renseignements personnels et les documents électroniques [16] ou lorsqu'une loi essentiellement similaire adoptée par une province canadienne s'applique dans le domaine privé. La loi fédérale s'applique aux renseignements personnels recueillis, utilisés ou communiqués dans le cadre d'activités commerciales, que celles-ci relèvent d'organisations telles que des associations, des sociétés de personnes, des personnes individuelles ou des organisations syndicales ou d'entreprises fédérales telles que des installations, des ouvrages, des entreprises ou des secteurs d'activité qui relèvent de la compétence législative du Parlement canadien. Les provinces du Québec, de la Colombie-Britannique et de l'Alberta ont adopté des lois essentiellement similaires à la loi fédérale; l'Ontario, le Nouveau-Brunswick, Terre-Neuve-et-Labrador et la Nouvelle-Écosse ont adopté des lois essentiellement similaires à la loi fédérale dans le domaine des renseignements sur la santé. Dans toutes les provinces du Canada, la loi fédérale s'applique à tous les renseignements personnels recueillis, utilisés ou communiqués par les entreprises fédérales, y compris les renseignements personnels au sujet des employés de celles-ci. La loi fédérale s'applique également aux

15 Mise à jour par le ch. I de l'O du 14 août 2024, en vigueur depuis le 15 sep. 2024 (RO **2024** 435).
16 La loi fédérale canadienne est disponible à l'adresse suivante: https://laws-lois.justice.gc.ca/fra/lois/P-8.6.textecomplet.html

renseignements personnels qui circulent d'une province ou d'un pays à l'autre dans le cadre d'activités commerciales.

8	Chypre***
9	Croatie***
10	Danemark*
11	Espagne*
12	Estonie*
13	Finlande*
14	France*
15	Gibraltar***
16	Grèce*
17	Guernesey***
18	Hongrie*
19	Île de Man***
20	Îles Féroé***
21	Irlande***
22	Islande*
23	Israël***
24	Italie*
25	Jersey***
26	Lettonie*
27	Liechtenstein*
28	Lituanie*
29	Luxembourg*
30	Malte*
31	Monaco***
32	Norvège*
33	Nouvelle-Zélande***
34	Pays-Bas*
35	Pologne*
36	Portugal*
37	Tchéquie*
38	Roumanie***

39	Royaume-Uni**	
40	Slovaquie*	
41	Slovénie*	
42	Suède*	
43	Uruguay***	
44	États-Unis***	Un niveau de protection adéquat est réputé garanti pour les données personnelles traitées par les organisations certifiées conformément aux principes du cadre de protection des données entre la Suisse et les États-Unis[17], en vertu des garanties octroyées par le décret exécutif 14086 du 7 octobre 2022[18], par le règlement du 7 octobre 2022 sur la cour d'examen en matière de protection des données du procureur général des États-Unis[19], par la directive 126 de la communauté du renseignement (procédures de mise en œuvre pour le mécanisme de recours en matière de renseignement selon le décret exécutif 14086) établie par le bureau de la directrice du renseignement national le 6 décembre 2022[20] et par la désignation de la Suisse le 7 juin 2024 en tant qu'État bénéficiant du mécanisme de recours à deux niveaux comprenant l'accès à la cour d'examen en matière de protection des données[21].

* L'évaluation du niveau de protection adéquat inclut les transferts de données selon la Directive (UE) 2016/680[22].

** L'évaluation du niveau de protection adéquat inclut les transferts de données en vertu d'une décision d'exécution de la Commission européenne constatant le caractère adéquat du niveau de protection des données selon la Directive (UE) 2016/680.

*** L'évaluation du niveau de protection adéquat n'inclut pas les transferts de données dans le cadre de la coopération prévue par la Directive (UE) 2016/680.

17 Les principes sont disponibles à l'adresse suivante: www.dataprivacyframework.gov/s/framework-text?tabset-c1491=3.

18 Le décret exécutif 14086 est disponible à l'adresse suivante: www.state.gov/executive-order-14086-policy-and-procedures/.

19 Le règlement est disponible à l'adresse suivante: www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court.

20 La directive est disponible à l'adresse suivante: www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.

21 La désignation est disponible à l'adresse suivante: www.justice.gov/opcl/media/1355326/dl?inline.

22 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, JO L 119 du 4.5.2016, p. 89.

Annexe 2[23]
(art. 45)

Abrogation et modification d'autres actes

I

L'ordonnance du 14 juin 1993 relative à loi fédérale sur la protection des données[24] est abrogée.

II

Les actes mentionnés ci-après sont modifiés comme suit:

…[25]

23 Mise à jour par l'annexe 6 ch. II 1 de l'O du 23 sept. 2022 sur l'analyse génétique humaine, en vigueur depuis le 1er sept. 2023 (RO **2022** 585).
24 [RO **1993** 1962; **2000** 1227 annexe ch. II 7; **2006** 2331 annexe 2 ch. 3, 4705 ch. II 24; **2007** 4993; **2008** 189; **2010** 3399]
25 Les mod. peuvent être consultées au RO **2022** 568 et 585 annexe 6 ch. II 1.