Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Office fédéral de la justice OFJ
Domaine de direction Droit public

Révision totale de la loi sur la protection des données : Foire aux questions

Date : février 2024
Référence du dossier : 212.9-754/50/4

La révision totale de la loi sur la protection des données (LPD ; RS 235.1 ; entrée en vigueur : 1er septembre 2023) vise à adapter la protection des données aux développements technologiques et à améliorer la compatibilité avec le droit européen. Le présent document rassemble diverses questions fondamentales auxquelles l'Office fédéral de la justice (OFJ) répond dans le but de permettre une meilleure compréhension de la nouvelle loi et de ses dispositions d'exécution, mais aussi de faciliter les travaux de mise en œuvre pour les organes fédéraux et les responsables du traitement privés.

Cette FAQ suit la systématique de la LPD. Les réponses s'appuient notamment sur le message du Conseil fédéral du 15 septembre 2017 relatif à la révision totale de la LPD ainsi que sur le rapport explicatif de l'OFJ du 31 août 2022 relatif à l'ordonnance sur la protection des données (OPDo ; RS 235.11 ; entrée en vigueur : 1er septembre 2023). Une attention particulière est cependant aussi accordée aux dispositions qui n'ont été introduites dans la nouvelle LPD que dans le cadre des délibérations parlementaires et pour lesquelles il n'existe donc jusqu'à présent que peu de documentation (p. ex., concernant la notion de « profilage à risque élevé » ou l'obligation de désigner un représentant qui incombe aux responsables du traitement privés ayant leur siège ou leur domicile à l'étranger).

Le présent document remplace la « FAQ Droit de la protection des données » de l'OFJ du 1er février 2023. Il sera constamment mis à jour et complété.

Table des matières

1. Champ d'application de la LPD

1.1 Champ d'application personnel et matériel

1.1.1 **Question** : *À qui s'applique la LPD (champ d'application personnel) ?*

La LPD s'applique aux *personnes privées* et aux *organes fédéraux* qui traitent des données personnelles (art. 2, al. 1, LPD). Selon l'art. 5, let. i, LPD, un organe fédéral est une autorité fédérale, un service fédéral ou une personne chargée d'une tâche publique de la Confédération. La notion de « personne privée » n'est, quant à elle, pas définie dans la loi. Il s'agit notamment d'entreprises ou de personnes physiques (pour autant qu'elles ne traitent pas des données dans le cadre de l'exécution d'une tâche publique).

Le traitement de données personnelles par les *autorités cantonales (et communales)* n'est pas régi par la LPD, mais par le droit cantonal pertinent, que les autorités concernées aient obtenu ces données directement ou au moyen d'un accès en ligne à une banque de données fédérale. Le traitement de données par des organes cantonaux en exécution du droit fédéral est également soumis à la législation cantonale. Certains domaines relevant de la compétence de la Confédération, comme celui des assurances sociales, sont régis par une réglementation spéciale en matière de protection des données qui s'applique non seulement aux autorités fédérales compétentes, mais aussi aux autorités cantonales chargées de l'exécution du droit fédéral. Toutefois, même là, la Confédération ne saurait empiéter sur les compétences cantonales en matière d'organisation.

Référence : Message du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 6565, p. 6577 et 6631 (ci-après : « Message concernant la révision totale de la LPD ») ; Rapport du Conseil fédéral du 22 décembre 2010 « Échange de données personnelles entre autorités fédérales et autorités cantonales » en exécution du postulat Lustenberger 07.3682, FF 2011 615.

1.1.2 **Question** : *Quelles données sont protégées par la LPD (champ d'application matériel) ?*

Le traitement de données des personnes morales est exclu du champ d'application matériel de la nouvelle LPD. Celle-ci ne régit plus que le traitement de données des *personnes physiques* (= données personnelles). Elle ne confère donc des droits qu'aux personnes physiques, et non aux personnes morales (art. 2, al. 1, LPD a contrario).

Les personnes morales restent protégées par d'autres dispositions de la législation suisse. On pense notamment au code civil (protection de la personnalité conférée par les art. 28 ss CC ; RS 210), à la loi fédérale contre la concurrence déloyale (LCD ; RS 241), à la loi sur le droit d'auteur (LDA ; RS 231.1) et aux règles sur les secrets professionnels, d'affaires et de fabrication. En outre, la sphère privée des personnes morales est garantie par l'art. 13 de la Constitution (Cst. ; RS 101). Cela signifie notamment que les organes fédéraux ne sont en droit de traiter ou de communiquer des données concernant des personnes morales que s'il existe une base légale suffisante. La révision totale de la LPD introduit donc dans la loi sur l'organisation du gouvernement et de l'administration plusieurs dispositions légales qui règlent la marche à suivre pour traiter des données concernant des personnes morales par les organes fédéraux (art. 57*r* ss LOGA ; RS 172.010). En outre, la disposition transitoire de l'art. 71 LPD permet d'éviter l'apparition de lacunes juridiques pendant cinq ans.

La LPD ne s'applique pas aux données non personnelles ni aux données anonymisées, qui ne sont de fait plus des données personnelles.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6631 ss ; note de l'OFJ d'octobre 2022 sur les principales modifications en vue de l'élaboration des bases légales concernant le traitement de données par les organes fédéraux (ci-après : « Note de l'OFJ sur la révision totale de la LPD »), p. 26 ss.

1.1.3 **Question** : *Quelles exceptions au champ d'application personnel et matériel la LPD prévoit-elle ?*

Conformément à l'art. 2, al. 2, la LPD ne s'applique pas :

- aux traitements de données personnelles effectués par une personne physique pour un usage exclusivement personnel (let. a) ;
- aux traitements de données personnelles effectués par les Chambres fédérales et les commissions parlementaires dans le cadre de leurs délibérations (let. b) ;
- aux traitements de données personnelles effectués par les bénéficiaires institutionnels au sens de l'art. 2, al. 1, de la loi du 22 juin 2007 sur l'État hôte (RS 192.12) qui jouissent en Suisse de l'immunité de juridiction (let. c).

  Exemple : CICR.

L'art. 2, al. 3, LPD régit le rapport entre droit de procédure et LPD pour *les procédures civiles, les procédures pénales, les procédures d'entraide judiciaire internationale ainsi que les procédures de droit public et administratif (à l'exception des procédures administratives de première instance*) : selon cette disposition, les traitements de données personnelles et les droits des personnes concernées obéissent au droit de procédure applicable lorsqu'il existe un lien direct avec une procédure. Le droit de procédure garantit alors la protection de la personnalité et des droits fondamentaux de toutes les personnes concernées. À propos des exceptions à la surveillance par le Préposé fédéral à la protection des données et à la transparence (PFPDT), voir l'art. 4, al. 2, let. c à e, LPD.

En ce qui concerne les *registres publics relatifs aux rapports de droit privé* tenus par des *autorités fédérales*, l'art. 2, al. 4, LPD prévoit qu'ils sont régis par les dispositions spéciales du droit fédéral applicable. C'est notamment le cas pour l'accès à ces registres et les droits des personnes concernées. Si ces dispositions ne contiennent aucune réglementation à ce sujet, la LPD s'applique. Les registres sont par ailleurs désormais soumis à la surveillance du PFPDT (art. 4, al. 1, LPD). Sont concernés le registre informatisé de l'état civil, Zefix, le registre des aéronefs de l'Office fédéral de l'aviation civile et les registres de l'Institut fédéral de la propriété intellectuelle (notamment les registres des marques, des brevets et des designs).

En revanche, les registres publics relatifs aux rapports de droit privé qui relèvent de la compétence des *cantons* sont soumis au droit cantonal en matière de protection des données (voir question 1.1.1), y compris lorsque ces données sont traitées en exécution du droit fédéral. Le droit cantonal ne doit toutefois pas empêcher l'application correcte et uniforme du droit privé fédéral, et en particulier du principe de la publicité des registres. Les registres cantonaux comprennent le registre foncier, le registre des bateaux, les registres cantonaux du commerce, les registres concernant la poursuite pour dettes et faillites et le registre public sur les pactes de réserves de propriété.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6633 ss.

1.2 Champ d'application territorial

Question : *Quel est le champ d'application territorial de la LPD ?*

Dans le cadre de la révision totale de la LPD, le Parlement a inséré une réglementation explicite sur le champ d'application territorial à l'art. 3. La distinction suivante est établie :

- Pour les *dispositions de protection des données relevant du droit privé et du droit pénal*, l'art. 3, al. 2, LPD se réfère de manière déclaratoire aux règles de conflit de normes existantes dans la loi fédérale sur le droit international privé (art. 139 LDIP ; RS 291) et dans le code pénal (art. 3 ss CP ; RS 311.0).

- Pour les *dispositions de protection des données relevant du droit public* (y compris la surveillance par le PFPDT), l'art. 3, al. 1, LPD prévoit que la loi s'applique aux états de fait qui déploient des effets en Suisse, même s'ils se sont produits à l'étranger. Cette réglementation n'a rien de nouveau en soi non plus. Selon la jurisprudence, les dispositions de protection des données relevant du droit public s'appliquent en effet déjà aux états de fait internationaux s'il existe un lien prépondérant avec la Suisse. Il s'agit donc ici d'une codification en droit public de la pratique des tribunaux concernant le principe de territorialité et le principe des effets.

Référence : ATF 138 II 346, consid. 3.3.

2. Définitions

2.1 Données personnelles et données personnelles sensibles

2.1.1 **Question** : *Qu'entend-on par données personnelles ?*

Toutes les informations concernant une personne physique identifiée ou identifiable constituent des données personnelles (art. 5, let. a, LPD). Les données concernant les personnes morales n'entrent plus dans le champ d'application de la LPD (pour plus de détails, voir question 1.1.2).

Pour le reste, la définition de « données personnelles » correspond en substance à celle de l'ancien droit. Est réputée identifiable la personne physique qui peut être identifiée, directement ou indirectement, c'est-à-dire par corrélation d'informations tirées des circonstances ou du contexte (numéro d'identification, données de localisation, éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale). L'identification peut résulter d'un seul élément (numéro de téléphone, d'immeuble, numéro AVS, empreintes digitales) ou du recoupement de plusieurs informations (adresse, date de naissance, état civil). La possibilité purement théorique qu'une personne soit identifiée n'est pas suffisante. Si l'identification nécessite des moyens tels que, selon le cours ordinaire des choses, aucun intéressé ne les mettra en œuvre, on ne peut guère parler de possibilité d'identification. Il convient de prendre en compte dans chaque cas d'espèce l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour identifier la personne. Le caractère raisonnable des moyens en question doit être évalué au regard de l'ensemble des circonstances, telles que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de leur évolution.

Références : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6639 s. ; ATF 136 II 508.

2.1.2 **Question** : *Qu'entend-on par données personnelles sensibles ?*

La notion de données personnelles sensibles (données sensibles) est définie de manière exhaustive à l'art. 5, let. c, LPD. Comme c'était déjà le cas jusqu'ici, il s'agit des données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales (ch. 1), sur la

santé, la sphère intime ou l'origine raciale (ch. 2), sur des poursuites ou sanctions pénales et administratives (ch. 5) et sur des mesures d'aide sociale (ch. 6).

La LPD totalement révisée étend la notion de données sensibles aux données suivantes :

- *données sur l'origine ethnique (art. 5, let. c, ch. 2, LPD)* : dans la jurisprudence du Tribunal fédéral relative à l'art. 261bis CP, une ethnie est définie comme un segment de la population qui se considère lui-même comme un groupe distinct et que le reste de la population perçoit également comme un groupe. Une ethnie doit avoir une histoire commune ainsi qu'un système commun et cohérent de valeurs et de normes comportementales (traditions, coutumes, usages, langue, etc.), ces caractéristiques devant être utilisées pour délimiter le groupe[1].

  Exemples : Albanais du Kosovo, Arabes, Palestiniens ou gens du voyage[2].

- *données génétiques (art. 5, let. c, ch. 3, LPD)* : les données génétiques sont les informations relatives au patrimoine génétique d'une personne obtenues par une analyse génétique. Cette définition correspond à l'art. 3, let. k, de la loi fédérale sur l'analyse génétique humaine (LAGH ; RS 810.12).

  Exemple : profil d'ADN.

- *données biométriques identifiant une personne physique de manière univoque (art. 5, let. c, ch. 4, LPD)* : on entend par données biométriques au sens de l'art. 5, let. c, ch. 4, LPD les données personnelles résultant d'un traitement technique spécifique et relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment son identification univoque. À la différence des données génétiques, ces données doivent impérativement résulter d'un traitement technique qui permet l'identification univoque de la personne concernée pour être considérées comme des données sensibles. Sans cette restriction, des photographies ou des enregistrements sonores ordinaires seraient également considérés comme telles.

  Exemples : photographies du visage traitées avec un logiciel de reconnaissance faciale, empreintes digitales, images de l'iris et de la rétine.

Le traitement de données sensibles n'est pas interdit. Il est cependant soumis à des conditions plus strictes que d'autres traitements de données. Ainsi, les exigences relatives à un éventuel consentement sont plus élevées (art. 6, al. 7, let. a, LPD). De plus, les organes fédéraux doivent généralement se fonder sur une base légale dans une loi au sens formel pour traiter de telles données (art. 34, al. 2, let. a, et 36, al. 1, LPD), et une analyse d'impact relative à la protection des données doit être établie lors du traitement de données sensibles à grande échelle (art. 22, al. 2, let. a, LPD).

Références : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6640 s. ; Note de l'OFJ sur la révision totale de la LPD, p. 10 s.

2.1.3 **Question** : *Toutes les données génétiques sont-elles des données sensibles ?*

Comme c'était déjà le cas dans l'ancien droit, seules les données concernant une personne physique identifiée ou identifiable entrent dans le champ d'application de la nouvelle LPD (art. 5, let. a, LPD ; voir question 2.1.1). En d'autres termes, les données génétiques ne constituent des données sensibles que si elles contiennent des informations qui permettent d'identifier assez aisément la personne concernée. Si tel n'est pas le cas, les données génétiques

[1] ATF 143 IV 193, consid. 2.3.

[2] Ces exemples proviennent de FABIENNE ZANNOL, Die Anwendung der Strafnorm gegen Rassendiskriminierung (étude sur mandat de la CFR), Berne, 2007.

n'entrent pas dans le champ d'application de la LPD. Celle-ci ne s'applique pas non plus aux données anonymisées lorsqu'une reconstitution de l'identité par un tiers n'est plus possible.

Références : BO 2019 N 1787 (intervention de la cheffe du DFJP lors du débat du 24 septembre 2019 sur la révision totale de la LPD devant le Conseil national).

2.2 Traitement

2.2.1 **Question** : *Qu'entend-on par « traitement » de données personnelles ?*

Selon l'art. 5, let. d, LPD, on entend par traitement toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données. La définition se veut neutre sur le plan technologique et englobe aussi bien le traitement automatisé que le traitement non automatisé (manuel) des données.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6641.

2.2.2 **Question** : *Qu'est-ce que le traitement « automatisé » de données ?*

La notion de traitement « automatisé » des données n'est pas définie dans la LPD, mais plusieurs dispositions de cette loi et de l'OPDo s'y réfèrent expressément (p. ex., art. 5, let. f, LPD sur la notion de profilage, art. 28 sur le droit à la remise ou à la transmission des données personnelles, art. 35 sur les essais pilotes, art. 4, al. 1 et 2, OPDo sur la journalisation et 5 et 6 sur le règlement de traitement). Le traitement automatisé des données doit être considéré comme le pendant du traitement manuel ou analogique (p. ex., rédaction d'une note manuscrite lors d'un entretien d'embauche). Il désigne tout traitement effectué sous forme électronique (p. ex., à l'aide d'un ordinateur, d'un smartphone, d'une tablette ou d'un appareil photo). Il n'est pas nécessaire que l'opération soit effectuée en totalité à l'aide de procédés automatisés — c'est-à-dire sans intervention humaine —, comme l'exige la notion de décision individuelle automatisée au sens de l'art. 21 LPD (voir question 6.2.1).

2.3 Profilage

2.3.1 **Question** : *Qu'entend-on par profilage ?*

La notion de « profil de la personnalité » (art. 3, let. d, aLPD) a été remplacée par celle de « profilage » (art. 5, let. f, LPD). Ces deux notions, bien que présentant de nombreuses similitudes, ne couvrent pas le même état de fait. Le profil de la personnalité est le résultat d'un traitement (= compilation de données fournissant une image sur des aspects [partiels] importants relatifs à une personne physique) et traduit ainsi quelque chose de statique. À l'inverse, le profilage désigne une forme ou une méthode particulière de traitement des données (= évaluation automatisée de certains aspects relatifs à une personne physique), et constitue donc un processus dynamique.

Selon l'art. 5, let. f, LPD, le profilage désigne toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique. Pour simplifier, le profilage consiste en une sorte d'appréciation ou d'évaluation d'une personne. Il peut servir pour analyser certaines caractéristiques de la personnalité, mais aussi pour prédire un comportement.

Le profilage ne consiste pas à établir objectivement un état de fait. Une simple répartition de personnes selon des caractéristiques connues telles que l'âge, le sexe ou la taille ne constitue pas un profilage tant qu'aucune prévision n'est faite ou qu'aucune conclusion n'est tirée concernant des individus.

Le traitement des données, et plus particulièrement le processus d'évaluation, se fait de manière automatisée dans le cas du profilage. À la différence d'une décision individuelle automatisée (voir question 6.2.1), il n'est toutefois pas nécessaire que l'opération soit effectuée en totalité à l'aide de procédés automatisés. En effet, l'intervention d'une personne n'exclut pas le profilage, tant que le traitement des données se fait essentiellement de façon automatisée.

Exemples [3]:

- *Évaluation de la situation économique ou de la solvabilité : le score de crédit (« credit scoring ») est une méthode mathématique et statistique permettant d'évaluer la solvabilité d'une personne et sa disposition à payer. Cette analyse inclut des informations concernant des mises aux poursuites, des actes de défaut de biens, un blocage de comptes bancaires et de cartes de crédit en raison de retards de paiement, des demandes de crédits, des procédures de paiement ou de recouvrement ou des expériences tirées d'anciennes relations d'affaires. La personne concernée se voit attribuer une notation de crédit (score), qui sera utilisée par exemple pour décider de l'octroi d'un prêt ou définir les modalités de paiement (achat contre facture). Si l'attribution du score se fait de manière automatisée (et non manuellement), il s'agit d'un profilage.*
- *Évaluation de la santé : si un dispositif de suivi de l'activité physique compte uniquement les pas, il n'y a en principe pas d'évaluation de la santé de la personne et donc pas de profilage. Si le comptage des pas est en revanche combiné avec d'autres données, par exemple la taille, le poids, le sexe, les habitudes alimentaires, le rythme de sommeil ou les données GPS, des analyses de l'état de santé sont possibles. Une telle analyse (automatisée) de la santé constitue un profilage.*

Références : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6641 s. ; Note de l'OFJ sur la révision totale de la LPD, p. 12 ss.

2.3.2 **Question** : *Quand parle-t-on de « profilage à risque élevé » ?*

La notion de « profilage à risque élevé » a été introduite durant les délibérations parlementaires sur la révision totale de la LPD. Le Parlement a opté pour une approche fondée sur le risque. Dès lors, le profilage issu du traitement de données par des responsables privés n'a de conséquences juridiques qualifiées que s'il est « à risque élevé ». Pour les organes fédéraux en revanche, la distinction entre profilage « ordinaire » et « à risque élevé » n'a que peu de conséquences (voir question 2.3.3).

Selon l'art. 5, let. g, LPD, le profilage à risque élevé désigne « tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique ». Cette définition correspond à celle de « profil de la personnalité » qui figurait à l'art. 3, let. d, aLPD. La jurisprudence relative au profil de la personnalité (en particulier l'arrêt principal du Tribunal administratif fédéral du 18 avril 2017 A-4232/2015) reste de ce fait déterminante.

En d'autres termes, il y a profilage à risque élevé lorsque son résultat est un profil de la personnalité au sens de l'ancienne LPD. Il s'agit par conséquent d'une combinaison entre méthode de traitement des données (profilage) et résultat du traitement des données (profil de la per-

[3] Ces exemples sont tirés d'Olivier Heuberger, *Profiling im Persönlichkeits— und Datenschutzrecht der Schweiz*, thèse, Lucerne, 2020 (ch. 157 ss).

sonnalité). Cette définition légale tient compte du fait qu'un grand nombre de données (y compris des données non sensibles) peuvent être appariées et donner une image de la personne concernée qui, elle, constitue un risque élevé pour les droits de la personnalité et les droits fondamentaux. La personne concernée n'a souvent aucun moyen d'influer sur cette image et ne peut contrôler ni son exactitude ni son utilisation.

Exemples :

- Le GPS intégré dans un smartphone permet en principe de localiser l'appareil à quelques mètres près. Le traitement des données de mouvement d'un smartphone peut être automatisé en vue de tirer des conclusions sur son propriétaire. Si ces données ne sont analysées que sur une courte durée et pour un endroit précis (p. ex. passage dans une gare), il n'y a généralement qu'un « profilage ordinaire ». Par contre, si les données de mouvement sont enregistrées sur une période plus longue, dans un rayon géographique plus étendu, elles permettent de tirer des conclusions sur toute une série de domaines de la vie d'une personne, comme le lieu de travail, les conditions de logement, les habitudes alimentaires, les relations personnelles, les éventuelles visites chez un médecin ou les habitudes de consommation. Il en résulte une image de la personne, qui mérite d'être spécialement protégée. Dans un tel cas, il y aurait un profilage à risque élevé.
- Un profilage pour vérifier la solvabilité qui ne se fonde pas uniquement sur la situation économique et la capacité de paiement de la personne concernée, mais inclut également des données sur d'autres aspects de sa personnalité (tels que les conditions de logement et la situation de vie) doit être qualifié de profilage à risque élevé (voir l'arrêt du Tribunal administratif fédéral du 18 avril 2017 A-4232/2015 rendu sous l'ancien droit).

Dans la pratique, le profilage peut entraîner de graves atteintes à la personnalité ou aux droits fondamentaux des personnes concernées pour d'autres motifs. On pense par exemple au profilage de mineurs ou d'autres personnes particulièrement vulnérables, ou encore au profilage pouvant donner lieu au refus d'une importante prestation. Il convient de tenir compte de ces risques lors de l'établissement d'une analyse d'impact relative à la protection des données personnelles au sens de l'art. 22 LPD (voir question 6.3.2).

Référence : Note de l'OFJ sur la révision totale de la LPD, p. 15 s.

2.3.3 **Question** : *Quelles sont les conséquences d'un profilage ordinaire et d'un profilage à risque élevé ?*

Les responsables du traitement privés sont soumis à des conditions plus rigoureuses pour un profilage à risque élevé que pour d'autres traitements de données. Ainsi, les exigences relatives à un éventuel consentement sont plus strictes (art. 6, al. 7, let. b, LPD). De même, lorsqu'un profilage à risque élevé est envisagé, une analyse d'impact relative à la protection des données doit en principe être réalisée (art. 22, al. 1 et 2, LPD ; voir question 6.3.2). Les organes fédéraux sont, quant à eux, déjà soumis à des conditions plus rigoureuses lorsqu'ils font du profilage « ordinaire ». Ils ne sont notamment autorisés à procéder à un profilage que si une loi au sens formel le prévoit (art. 34, al. 2, let. b, LPD).

2.3.4 **Question** : *Les responsables du traitement privés ont-ils forcément besoin du consentement de la personne concernée pour procéder à un profilage ? Qu'en est-il pour les organes fédéraux ?*

Les *responsables du traitement privés* ne sont en principe autorisés à procéder à un profilage — ou à tout autre type de traitement de données — que si celui-ci ne porte pas une atteinte illicite à la personnalité des personnes concernées (art. 30, al. 1, LPD). Notons que le profilage n'est pas considéré par la LPD comme un type de traitement de données constituant en soi une atteinte à la personnalité (art. 30, al. 2, LPD a contrario). Un profilage qui, dans une certaine mesure, porte atteinte à la personnalité de la personne concernée, peut toutefois être justifié par le consentement de cette personne, mais aussi par un intérêt privé ou public

prépondérant, ou par la loi (art. 31, al. 1, LPD). L'obtention du consentement n'est donc pas toujours requise, y compris en cas d'atteinte à la personnalité. Il est en effet possible de faire valoir les autres motifs justificatifs mentionnés, notamment un intérêt privé ou public prépondérant (voir entre autres art. 31, al. 2, LPD). Ainsi, la lutte contre la fraude pourrait être invoquée comme un intérêt légitime à un profilage si, dans un cas d'espèce, cet intérêt l'emporte sur ceux, contraires, de la personne concernée.

Lorsque le consentement de la personne concernée est utilisé comme motif justificatif à un profilage portant atteinte à la personnalité, il doit satisfaire aux exigences de l'art. 6, al. 6, LPD ou, dans le cas d'un profilage à risque élevé, à celles de l'art. 6, al. 7, let. b, LPD (à propos des exigences relatives au consentement, voir question 3.4.2).

Contrairement aux responsables du traitement privés, les *organes fédéraux* ne sont, en vertu du principe de la légalité, en droit de traiter des données personnelles que si une base légale le prévoit (art. 34, al. 1, LPD). L'art. 34, al. 2, let. b, LPD exige même une base légale dans une loi au sens formel pour le profilage. La LPD prévoit plusieurs exceptions à cette exigence s'il n'y a pas de base légale. Parmi celles-ci figure le consentement de la personne concernée dans le cas d'espèce (art. 34, al. 4, let. b, LPD). Le consentement revêt une importance bien moindre dans le traitement de données par des organes fédéraux que dans celui par des personnes privées. En effet, le traitement régulier ou durable de données personnelles ne saurait être justifié par le consentement des personnes concernées. Il convient plutôt de créer les bases légales nécessaires.

3. Principes (sélection)

3.1 Principe de la transparence et de la reconnaissabilité

Question : *Qu'est-ce que le principe de la transparence et de la reconnaissabilité ?*

Le principe de la transparence et de la reconnaissabilité découle de l'art. 6, al. 3, LPD. Même si le libellé de cet article s'éloigne quelque peu de l'ancienne disposition (art. 4, al. 4, aLPD), aucun changement matériel n'est prévu, comme expliqué dans le message concernant la révision totale de la LPD. La collecte de données personnelles, et en particulier la finalité de cette collecte, doit être reconnaissable pour la personne concernée. C'est en principe le cas lorsque la personne est informée, lorsque le traitement est prévu par une loi ou qu'il ressort clairement des circonstances.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, 6644 s.

3.2 Principe de la finalité

Question : *Qu'est-ce que le principe de la finalité ?*

L'art. 6, al. 3, LPD concernant le principe de la finalité est formulé quelque peu différemment de l'ancien droit (art. 4, al. 3, aLPD). La nouvelle disposition indique clairement que les données personnelles ne peuvent être traitées que de manière compatible avec les finalités pour lesquelles elles ont été collectées en premier lieu. Cette nouvelle formulation n'apporte toutefois pas de changements majeurs : comme auparavant, un traitement ultérieur de données personnelles va à l'encontre du principe de la finalité si la personne concernée peut légitimement le considérer comme inattendu, inapproprié ou contestable.

Exemples :

- Le fait d'utiliser à des fins publicitaires des adresses obtenues dans le cadre de la récolte de signatures pour une initiative populaire n'est pas compatible avec les finalités initiales.

- Si la personne concernée transmet son adresse pour obtenir une carte client ou pour une commande, l'utilisation ultérieure de cette adresse à des fins commerciales par l'entreprise elle-même correspond à une finalité de traitement reconnaissable et qui est donc compatible avec les finalités initiales[4].

Une modification du but initial est admise lorsqu'elle est prévue par la loi, requise par un changement législatif, ou légitimée par un autre motif justificatif (p. ex. le consentement de la personne concernée).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, 6645.

3.3 Principe de l'exactitude

Question : *Qu'exige le principe de l'exactitude des données ?*

Celui qui traite des données personnelles doit s'assurer qu'elles sont exactes (art. 6, al. 5, 1re phrase, LPD). Il prend toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées (art. 6, al. 5, 2e phrase, LPD). À la troisième phrase de l'art. 6, al. 5 de la nouvelle LPD, le Parlement a également précisé que le caractère approprié de la mesure dépend notamment du type de traitement et de son étendue, ainsi que du risque que le traitement des données en question présente pour la personnalité ou les droits fondamentaux des personnes concernées. Cet ajout permet d'inscrire dans la loi ce qui était déjà admis jusqu'ici par la doctrine et la pratique (en particulier celle du Tribunal administratif fédéral) en matière d'exactitude des données. Il n'implique toutefois pas de changements sur le plan matériel.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, 6646 s.

3.4 Consentement

3.4.1 Question : *Est-il nécessaire d'obtenir le consentement de la personne concernée pour pouvoir traiter ses données personnelles ?*

Le traitement de données personnelles par des *personnes privées* est en principe autorisé sans le consentement de la personne concernée. Le consentement n'est nécessaire que lorsqu'il sert à justifier un traitement de données portant atteinte à la personnalité (art. 30 s. LPD). Un traitement peut par exemple porter atteinte à la personnalité si des données sensibles (données relatives à la santé ; voir question 2.1.2) sont communiquées à des tiers (art. 30, al. 2, let. c, LPD). Si le consentement est nécessaire, il doit remplir les exigences fixées à l'art. 6, al. 6 et 7, LPD (voir question 3.4.2). Un traitement de données portant atteinte à la personnalité n'est toutefois pas automatiquement interdit s'il n'a pas été possible d'obtenir le consentement de la personne concernée, ou si le consentement n'est pas valable ou qu'il a été révoqué. En effet, il est possible de faire valoir d'autres motifs justificatifs tels que l'existence d'une base légale ou d'un intérêt public ou privé prépondérant.

Lorsque les données sont traitées par des *organes fédéraux*, le consentement de la personne concernée revêt moins d'importance que dans le domaine du droit privé. Dans ce cas-ci, c'est avant tout l'exigence d'une base légale qui est importante (art. 34 ss LPD). Le consentement peut exceptionnellement servir de base à un traitement par des organes fédéraux dans un cas particulier (art. 34, al. 4, let. b et 36, al. 2, let. b, LPD).

Au sujet de l'importance du consentement en cas de profilage, voir la question 2.3.4.

[4] PHILIPPE MEIER, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, N 731.

3.4.2 **Question** : *Quels critères le consentement doit-il remplir ?*

Si le consentement de la personne concernée est requis (voir question 3.4.1), il est uniquement valable, conformément à l'art. 6, al. 6, LPD, si celle-ci exprime librement sa volonté concernant un ou plusieurs traitements déterminés et qu'elle a été dûment informée. Le fait que le Parlement ait supprimé l'exigence du caractère « clair » du consentement, qui figurait encore dans le projet du Conseil fédéral, n'implique aucun changement matériel. Selon les principes généraux de l'ordre juridique en vigueur en Suisse, pour que le consentement soit valable, il faut toujours qu'il soit suffisamment clair.

L'art. 6, al. 7, LPD dresse la liste des cas dans lesquels le consentement (une fois encore, seulement lorsqu'il est requis) doit satisfaire à des exigences plus élevées et qu'il doit être formulé expressément. Il s'agit des cas suivants : le traitement de données sensibles (let. a), le profilage à risque élevé effectué par une personne privée (let. b), et le profilage effectué par un organe fédéral (let. c). On considère que le consentement est exprès lorsqu'il résulte d'une action ; il ne peut pas être tacite ou implicite. Il doit manifester clairement la volonté de la personne concernée.

Exemples :

- Un consentement écrit ou oral est exprès, tout comme des gestes tels que des signes approbateurs de la tête ou un signe de la main univoque. Sur Internet, le fait de cliquer sur une case et de la cocher est également considéré comme un consentement exprès.

- En revanche, un consentement implicite, comme le fait de continuer à utiliser un service après avoir été informé de changements dans les conditions générales, n'est pas exprès.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, 6646 s.

3.4.3 **Question** *: La LPD entièrement révisée prévoit-elle une interdiction de coupler la fourniture d'une prestation au traitement de données personnelles ?*

L'art. 7, par. 4 du Règlement général sur la protection des données de l'UE (voir question 12.2.1) instaure une interdiction de coupler la fourniture d'une prestation au traitement de données personnelles. Cela signifie que si un contrat dépend du consentement à un traitement de données qui n'est pas nécessaire à l'exécution dudit contrat, on part du principe que le consentement n'a pas été donné librement et qu'il n'est donc pas valable.

Contrairement à ce qui est prévu dans le RGPD, la LPD n'instaure pas une telle interdiction. Conformément aux dispositions suisses en matière de protection des données, il faut toutefois que le consentement soit exprimé librement. Lorsqu'une personne donne son consentement parce qu'elle s'expose à des désavantages qui ne sont aucunement liés à l'objectif du traitement des données ou qui sont disproportionnés en cas de refus, elle ne le donne pas librement. En soi, ce principe poursuit le même objectif que l'interdiction de couplage. En conclusion, en Suisse également il faut rigoureusement examiner les cas de couplage au moment de déterminer si le consentement est donné librement ou non.

Référence : ATF 138 I 331 consid. 7.4.1.

3.5 Protection des données dès la conception et par défaut

Question : *Qu'est-ce que la protection des données dès la conception (privacy by design) et par défaut (privacy by default) ?*

La protection des données dès la conception (*privacy by design* ; art. 7, al. 1 et 2 LPD) signifie que le responsable du traitement doit, dès la conception du traitement, mettre en place des mesures techniques et organisationnelles afin de respecter les prescriptions de protection des données. En d'autres termes, pour être conforme à la protection des données, un traitement doit s'effectuer dans un système remplissant déjà les exigences légales, de manière à rendre impossible une violation de la protection des données ou d'en réduire la probabilité.

Exemple : Une application est programmée afin que les données personnelles soient effacées régulièrement ou anonymisées systématiquement.

Les responsables sont également tenus de garantir, par le biais de préréglages appropriés (*privacy by default* ; art. 7, al. 3, LPD) que le traitement des données personnelles soit limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, 6648 ss.

3.6 Sécurité des données

3.6.1 Généralités

3.6.1.1 **Question** : *Qu'est-ce qu'une violation de la sécurité des données ?*

Conformément à l'art. 8, al. 1, LPD, les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru. Ces mesures doivent permettre d'éviter toute violation de la sécurité des données (art. 8, al. 2, LPD).

L'art. 5, let. h, LPD définit la violation de la sécurité des données : il s'agit de toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données. Ce qui compte, c'est qu'une violation se soit produite. Peu importe que la divulgation ou l'accès non autorisé aient simplement été rendus possibles ou se soient effectivement produits.

Au sujet de l'obligation d'annoncer les violations de la sécurité des données, voir le ch. 6.4.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, 6642 s. et 6651.

3.6.1.2 **Question** : *Que doivent faire les responsables du traitement et les sous-traitants pour assurer une sécurité adéquate des données personnelles ?*

En application de l'art. 8, al. 3, LPD, le Conseil fédéral a fixé aux art. 1 à 6 OPDo les exigences minimales en matière de sécurité des données.

De manière très générale, pour assurer une sécurité adéquate des données, les responsables du traitement et les sous-traitants doivent établir le *besoin de protection des données personnelles* et déterminer les *mesures techniques et organisationnelles* appropriées par rapport au *risque* encouru (art. 1, al. 1, OPDo).

- Pour établir le *besoin de protection des données personnelles*, il faut évaluer le type de données traitées ainsi que la finalité, la nature, l'étendue et les circonstances du traitement (art. 1, al. 2, OPDo).

  Pour déterminer le *risque pour la personnalité ou les droits fondamentaux de la personne concernée*, il faut évaluer les causes du risque, les principales menaces, les mesures prises ou prévues pour réduire le risque ainsi que la probabilité et la gravité d'une violation de la sécurité des données, malgré les mesures prises ou prévues (art. 1, al. 3, OPDo).

- Pour déterminer *les mesures techniques et organisationnelles* nécessaires, il faut également prendre en compte l'état des connaissances et les coûts de mise en œuvre (art. 1, al. 4, OPDo).

L'art. 2 OPDo énonce les objectifs des mesures techniques et organisationnelles visant à garantir la sécurité des données. En fonction du besoin de protection, les responsables du traitement et les sous-traitants doivent prendre des mesures pour que les données traitées :

- ne soient accessibles qu'aux personnes autorisées (*confidentialité*) ;
- soient disponibles en cas de besoin (*disponibilité*) ;
- ne puissent pas être modifiées sans droit ou par mégarde (*intégrité*) ; et qu'elles
- soient traitées de manière à être traçables (*traçabilité*).

L'art. 3 OPDo dresse une liste de mesures qui peuvent permettre d'atteindre les objectifs fixés à son art. 2.

Au sujet de la journalisation au sens de l'art. 4 OPDo, voir les questions ch. 3.6.2.

Au sujet du règlement de traitement au sens de l'art. 5 s. OPDo, voir les questions ch. 3.6.2

Référence : Rapport explicatif de l'OFJ du 31 août 2022 relatif à l'ordonnance sur la protection des données (ci-après : « Rapport explicatif relatif à l'OPDo »), p. 18 ss.

3.6.2 Journalisation

3.6.2.1 **Question**: *Quels sont le sens et le but de l'obligation de journalisation ?*

La journalisation est une mesure visant à garantir la sécurité des données conformément à l'art. 3 OPDo. Elle constitue en outre une mesure classique de prévention en matière de cybersécurité.

L'objectif de la journalisation est de pouvoir vérifier le traitement des données personnelles a posteriori. En d'autres termes, elle permet de déterminer si des données ont été perdues, effacées, détruites, modifiées ou divulguées. Elle peut également fournir des renseignements permettant de savoir si les données personnelles ont été traitées conformément aux finalités. Elle sert en outre à déceler et à faire la lumière sur les violations de la sécurité des données (voir question 3.6.1.1). Elle n'est en revanche pas destinée à surveiller la façon dont les utilisateurs traitent les données personnelles.

Référence : Rapport explicatif relatif à l'OPDo, p. 26 ss.

3.6.2.2 **Question**: *Dans quels cas les responsables du traitement et les sous-traitants privés doivent-ils journaliser les traitements ?*

Les responsables du traitement et les sous-traitants privés doivent au moins journaliser les opérations d'enregistrement, de modification, de lecture, de communication, d'effacement

et de destruction des données lorsqu'ils procèdent à des traitements automatisés (voir question 2.2.2) de données sensibles (voir question 2.1.2) à grande échelle (voir question 3.6.2.3) ou à un profilage à risque élevé (voir question 2.3.2) et que les mesures préventives ne suffisent pas à garantir la protection des 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 (art. 4, al. 1, 2e phrase, OPDo).

Référence : Rapport explicatif relatif à l'OPDo, p. 26.

3.6.2.3 **Question** : *Qu'est-ce qu'un traitement de données sensibles « à grande échelle » ?*

L'expression « à grande échelle » figurant à l'art. 4, al. 1, OPDo (et d'autres dispositions telles que l'art. 22, al. 2, let. a, LPD, en ce qui concerne l'analyse d'impact relative à la protection des données personnelles, ou l'art. 5, al. 1, let. a, OPDo concernant le règlement de traitement, ou l'art. 24, let. a, OPDo concernant le registre des activités de traitement) se rapporte aux cas où des données sensibles ne sont pas simplement traitées de façon isolée. Il peut par exemple s'agir du traitement de données de patients par un cabinet médical ou un hôpital. En revanche, le traitement isolé de données d'un collaborateur absent pour cause de maladie par une entreprise ne constitue pas un traitement à grande échelle. On est en présence d'un traitement à grande échelle notamment lorsque le traitement de données sensibles constitue l'essentiel des activités de la personne ou de l'organe en question.

3.6.2.4 **Question** : *Dans quels cas les organes fédéraux doivent-ils journaliser les traitements de données ?*

Les organes fédéraux et leurs sous-traitants doivent au moins journaliser l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données en cas de traitement automatisé de données personnelles (voir question 2.2.2) (art. 4, al. 2, OPDo). Il s'agit des mêmes opérations que celles imposées aux responsables du traitement privés (voir question 3.6.2.2). Le champ d'application est toutefois plus large : l'obligation de journalisation vaut pour tous les traitements automatisés, qu'il s'agisse de données sensibles ou de profilage à risque ou non. Cela permet de respecter les exigences de l'art. 25 de la directive (UE) 2016/680 (voir question 12.1). Pour les traitements de données qui ne relèvent pas du champ d'application de la directive (UE) 2016/680, l'art. 46, al. 1, OPDo prévoit une période de transition de trois ans à partir de l'entrée en vigueur de la LPD ou au plus tard à la fin du cycle de vie du système. Dans l'intervalle, les dispositions de l'art. 4, al. 1, OPDo concernant les responsables du traitement privés s'appliquent également pour les organes fédéraux.

Référence : Rapport explicatif relatif à l'OPDo, p. 27 et 59.

3.6.2.5 **Question** : *Quelles sont les particularités de la journalisation lorsqu'il s'agit de données personnelles généralement accessibles au public ?*

D'après l'art. 4, al. 3, OPDo, en présence de données personnelles généralement accessibles au public, il faut au moins journaliser l'enregistrement, la modification, l'effacement et la destruction des données, *mais pas* la lecture et la communication.

Exemple : La consultation ou la lecture de l'annuaire fédéral, qui est accessible au public, ne doit pas obligatoirement être journalisée.

Référence : Rapport explicatif relatif à l'OPDo, p. 27

3.6.2.6 **Question** : *Qu'est-ce qui doit être journalisé ?*

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, le cas échéant, l'identité du destinataire des données (art. 4, al. 4, OPDo).

Référence : Rapport explicatif relatif à l'OPDo, p. 27

3.6.2.7 **Question** : *Pendant combien de temps et de quelle manière les procès-verbaux de journalisation doivent-ils être conservés ?*

Les procès-verbaux de journalisation doivent être conservés durant au moins un an, séparément du système dans lequel les données personnelles sont traitées (art. 4, al. 5, 1re phrase, OPDo). Pour les organes fédéraux, des prescriptions spéciales sont réservées (p. ex. art. 4, al. 1, let. b de l'ordonnance sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération ; RS 172.010.442). La durée de conservation doit toujours être proportionnée à la finalité de la sécurité des données. La conservation séparée du système est nécessaire, car sinon le procès-verbal lui-même pourrait être manipulé ou chiffré en cas de cyberattaques.

Les procès-verbaux doivent uniquement être accessibles aux organes ou personnes chargées 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 (il s'agit par exemple également des administrateurs du système, s'ils soupçonnent une faille de sécurité). Ils ne peuvent être utilisés qu'à cette fin (art. 4, al. 5, 2e phrase, OPDo). Ces données ne peuvent pas être utilisées dans un but de surveillance, notamment du comportement professionnel des utilisateurs. Une utilisation à des fins prévues par une loi spéciale, comme l'utilisation dans le cadre d'une procédure pénale, reste réservée.

Référence : Rapport explicatif relatif à l'OPDo, p. 27 s.

3.6.3 Règlement de traitement

3.6.3.1 **Question** : *Quand les responsables du traitement privés doivent-ils établir un règlement de traitement ?*

Les responsables du traitement privés et leurs sous-traitants doivent établir un règlement pour les traitements automatisés quand ils portent sur des données sensibles à grande échelle (voir question 3.6.2.3) ou en cas de profilage à risque élevé (voir question 2.3.2) (art. 5, al. 1, OPDo).

Référence : Rapport explicatif relatif à l'OPDo, p. 28 s.

3.6.3.2 **Question** : *Quand les organes fédéraux doivent-ils établir un règlement de traitement ?*

Conformément à l'art. 6, al. 1, OPDo, les organes fédéraux et leurs sous-traitants doivent établir un règlement pour les traitements automatisés lorsqu'ils traitent des données sensibles (let. a, voir question 2.1.2), qu'ils effectuent un profilage (let. b, voir question 2.3.1), lorsque la finalité ou le mode du traitement de données personnelles est susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée (let. c), lorsqu'ils permettent aux cantons, aux autorités étrangères, aux organisations internationales ou aux personnes privées

d'accéder aux données personnelles (let. d), lorsqu'il s'agit d'ensembles de données interconnectés (let. e), ou qu'ils exploitent un système d'information ou de gestion d'ensembles de données conjointement avec d'autres organes fédéraux (let. f).

Référence : Rapport explicatif relatif à l'OPDo, p. 29 s.

3.6.3.3 **Question** : *Que doit contenir le règlement de traitement ?*

Le règlement de traitement doit notamment contenir des informations sur l'organisation interne (p. ex. description de l'architecture du système), sur les procédures de traitement et de contrôle des données (p. ex. concernant la minimisation des données, la communication de données, la procédure d'exercice du droit d'accès et du droit à la remise ou à la transmission des données personnelles) ainsi que sur les mesures visant à garantir la sécurité des données (art. 5, al. 2 et 6, al. 2, OPDo). Par ailleurs, le règlement de traitement doit être actualisé régulièrement et être mis à disposition du conseiller à la protection des données (dans le domaine privé : s'il y en a un)(art. 5, al. 3 et 6, al. 3, OPDo, voir question 3.7).

Comme c'était déjà le cas, le règlement de traitement devra être conçu à la manière d'une documentation ou d'un manuel.

Référence : Rapport explicatif relatif à l'OPDo, p. 29 ss.

3.6.3.4 **Question** : *Quelle est la différence entre le règlement de traitement au sens des art. 5 s. OPDo et le registre des activités de traitement au sens de l'art. 12 LPD ?*

Voir à ce sujet la question 3.8.2.

3.7 Conseiller à la protection des données

3.7.1 **Question** : *Qui doit nommer un conseiller à la protection des données ?*

Les *responsables du traitement privés* ne sont pas obligés de nommer un conseiller à la protection des données. Ils peuvent toutefois le faire volontairement (art. 10, al. 1, LPD) et, dans certaines conditions (voir à ce sujet la question 3.7.3) profiter d'allégement en ce qui concerne l'analyse d'impact relative à la protection des données personnelles (ils peuvent renoncer à consulter le PFPDT [voir à ce sujet la question 6.3.3] ; art. 10, al. 3 en rel. avec art. 23, al. 4, LPD).

Les *organes fédéraux* sont quant à eux obligés de désigner un conseiller à la protection des données (art. 10, al. 4, LPD en rel. avec art. 25 OPDo). Plusieurs organes fédéraux peuvent désigner conjointement un conseiller. Cela vise surtout à permettre aux plus petits organes ou aux départements avec une structure organisationnelle centralisée d'utiliser des synergies et de faire des économies.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, 6652 ss ; Rapport explicatif relatif à l'OPDo, p. 50.

3.7.2 **Question** : *Quelles sont les tâches du conseiller à la protection des données ?*

Le conseiller participe à l'application des prescriptions relatives à la protection des données. Il contrôle les traitements de données et propose des mesures correctives lorsqu'une violation des dispositions relatives à la protection des données est constatée. Par ailleurs, il forme et conseille les collaborateurs en matière de protection des données (p. ex. lors de l'établissement de l'analyse d'impact relative à la protection des données ; voir question 6.3.1). Le conseiller sert par ailleurs d'interlocuteur pour les personnes concernées et pour les autorités

compétentes en matière de protection des données (à savoir, le PFPDT ; à ce sujet, en ce qui concerne les responsables du traitement privé, voir art. 10, al. 2, LPD, et en ce qui concerne les organes fédéraux, art. 10, al. 4, LPD en rel. avec les art. 26, al. 2 et 28 OPDo). La responsabilité d'assurer le respect de la protection des données incombe au seul responsable du traitement et non au conseiller à la protection des données.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, 6652 ss ; Rapport explicatif relatif à l'OPDo, p. 50 ss.

3.7.3 **Question** : *À quelles exigences est soumis le conseiller à la protection des données ?*

Conformément à l'art. 26, al. 1, OPDo, les conseillers à la protection des données des *organes fédéraux* doivent disposer des connaissances professionnelles nécessaires (let. a) et exercer leur fonction de manière indépendante par rapport à l'organe fédéral et sans recevoir d'instruction de celui-ci (let. b). Il faut garantir que le conseiller puisse formuler ses recommandations librement, sans avoir à craindre de préjudices. Son indépendance doit surtout être garantie par le biais de mesures organisationnelles : il faut éviter que la fonction de conseiller à la protection des données ait un impact négatif sur l'évaluation du collaborateur concerné.

Si les *responsables du traitement privés* veulent profiter d'un allégement eu égard à l'analyse d'impact (pas d'obligation de consulter le PFPDT [voir à ce sujet la question 6.3.3 ; art. 10, al. 3 en rel. avec art. 23, al. 4, LPD]), il faut que leur conseiller à la protection des données remplisse les mêmes conditions que celles prévues pour les conseillers des organes fédéraux (art. 10, al. 3, let. a et b, LPD). En revanche, il est précisé que le conseiller ne peut pas exercer des tâches incompatibles avec sa mission (art. 10, al. 3, let. b, LPD), ce qui pourrait être le cas, par exemple, s'il était membre de la direction, s'il exerçait des fonctions dans les domaines de la conduite du personnel ou de la gestion des systèmes informatiques, ou s'il appartenait à un service qui traite des données personnelles sensibles. Rien n'interdit en revanche d'imaginer qu'un conseiller à la protection des données puisse être en même temps délégué à la sécurité de l'information. Les responsables du traitement doivent publier les coordonnées de leur conseiller et les communiquer au PFPDT (art. 10, al. 3, let. d, LPD).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, 6652 ss ; Rapport explicatif relatif à l'OPDo, p. 50 ss.

3.7.4 **Question** : *Quelles obligations le responsable du traitement a-t-il vis-à-vis de son conseiller à la protection des données ?*

Les *organes fédéraux* doivent donner accès à leur conseiller à la protection des données à tous les renseignements, documents, registres des activités de traitement (voir à ce sujet la question 3.8.1) et à toutes les données personnelles dont il a besoin pour l'accomplissement de ses tâches (art. 27, al. 1, let. a, OPDo). Les bases légales spéciales qui empêcheraient le conseiller d'accéder à certaines informations sont réservées. Par ailleurs, les organes fédéraux doivent veiller (p. ex. par le biais de directives) à ce que le conseiller soit informé de toute violation de la sécurité des données (voir à ce sujet la question 3.6.1.1)(art. 27, al. 1, let. b, OPDo). Ce devoir concerne toutes les violations, et pas uniquement celles qui doivent être annoncées au PFPDT en vertu de l'art. 24 LPD. Le conseiller à la protection des données conseille le responsable du traitement pour savoir si la violation doit être annoncée au PFPDT conformément à l'art. 24 LPD (voir à ce sujet les questions 6.4.2 et 6.4.5). Il revient toutefois au responsable du traitement de se charger de l'annonce : c'est lui qui décide si des violations doivent être annoncées au PFPDT, et si oui, lesquelles. Enfin, l'organe fédéral doit publier les coordonnées du conseiller à la protection des données en ligne et les communiquer au PFPDT (art. 27, al. 2,

OPDo). Pour une publication sur Internet, il suffit d'indiquer l'adresse électronique de l'organe compétent (). Il n'est pas nécessaire de rendre public le nom du conseiller.

L'art. 23 OPDo prévoit également des obligations pour *les responsables du traitement privés* : ils doivent mettre les ressources nécessaires à la disposition de leur conseiller à la protection des données (let. a) ; lui donner accès à tous les renseignements, les documents, les registres des activités de traitement (voir question 3.8.1) et à toutes les données personnelles dont il a besoin pour l'accomplissement de cette tâche (let. b) et lui donner le droit d'informer l'organe supérieur de direction ou d'administration dans les cas importants (let. c).

Référence : Rapport explicatif relatif à l'OPDo, p. 48 et 51 s.

3.8 Registre des activités de traitement

3.8.1 **Question** : *Qu'est-ce qu'un registre des activités de traitement ?*

Selon l'art. 12, al. 1, LPD, les responsables du traitement et les sous-traitants tiennent chacun un registre de leurs activités de traitement. Le registre fournit les indications importantes relatives aux traitements de données d'un responsable du traitement ou d'un sous-traitant. En d'autres termes, il s'agit d'un descriptif général des activités de traitement. Il permet de savoir de manière assez précise si le traitement des données est conforme ou non aux principes de protection des données. Ce n'est *pas* un journal détaillé dans lequel figurent des informations précises concernant les traitements effectués à la manière d'un procès-verbal.

L'obligation de tenir un registre remplace l'obligation de déclarer les fichiers qui figurait dans l'ancienne loi (art. 11*a,* aLPD).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, 6655 ss.

3.8.2 **Question** : *Quelle est la différence entre le registre des activités de traitement au sens de l'art. 12 LPD et le règlement de traitement au sens des art. 5 s. OPDo ?*

Il faut bien distinguer le règlement de traitement (mesure permettant de garantir la sécurité des données prévue aux art. 5 s. OPDo ; voir à ce sujet le ch. 3.6.3) du registre des activités de traitement (art. 12 LPD). Alors que le registre des activités de traitement fournit un aperçu des traitements effectués par un responsable privé ou un organe fédéral, le règlement de traitement définit l'organisation interne (p. ex. l'architecture et l'exploitation des systèmes d'information ou la garantie des droits des personnes concernées), les procédures de traitement et de contrôle des données (p. ex. droits d'accès) ainsi que les mesures (techniques et organisationnelles) visant à garantir la sécurité des données (voir à ce sujet la question 3.6.3.3)

3.8.3 **Question** : *Qu'est-ce qui doit figurer dans le registre des activités de traitement ?*

L'art. 12, al. 2, LPD précise les indications minimales que doit contenir le registre des activités de traitement du responsable du traitement privé. Il s'agit de l'identité (le nom ou l'entreprise et l'adresse) du responsable du traitement (let. a), et de la finalité du traitement (let. b). Le registre doit également donner une description des catégories de personnes concernées (p. ex. « consommateurs » ou « employés ») et des catégories de données personnelles traitées (p. ex. « coordonnées » ou « détails de paiement »)(let. c). Il doit encore indiquer les catégories de destinataires auxquels les données sont susceptibles d'être communiquées (let. d). On parle de groupes types ayant des caractéristiques communes, p. ex. « autorités de surveillance », « fournisseurs » ou « prestataires de services informatiques ». Si les destinataires sont à l'étranger, le registre doit également mentionner le nom de l'État et les éventuelles ga-

ranties prises selon l'art. 16, al. 2, LPD (p. ex. clauses contractuelles types ; voir question 5.3.2) (let. g). Le registre doit aussi contenir le délai de conservation des données personnelles (let. e). S'il n'est pas possible de fournir une indication précise, le registre doit au moins indiquer les critères selon lesquels le délai est fixé. Conformément à l'art. 12, al. 2, let. f, LPD, le registre doit contenir une description générale des mesures visant à garantir la sécurité des données selon l'art. 8 OPDo (voir les questions ch. 3.6). La mention « dans la mesure du possible » indique que cette obligation ne s'applique que si les mesures peuvent être définies de façon suffisamment concrète.

L'art. 12, al. 3, LPD contient une liste plus courte des indications minimales qui doivent figurer sur le registre des activités de traitement du sous-traitant.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6655 ss.

3.8.4 **Question** : *Le registre des activités de traitement doit-il être déclaré au PFPDT ?*

Conformément à l'art. 12, al. 4, LPD, les *organes fédéraux* doivent déclarer leur registre d'activités de traitement au PFPDT. Celui-ci possède un portail d'annonce, c'est-à-dire un registre des activités de traitement qui est public (art. 56 LPD ; <https://datareg.edoeb.admin.ch>).

Cette obligation ne s'applique pas aux *responsables du traitement privés* (contrairement à ce que prévoyait l'ancien droit). En cas d'enquête (et sur demande du PFPDT), ceux-ci sont toutefois tenus, dans le cadre de leur obligation de collaboration, de le laisser accéder à leurs registres des activités de traitement afin qu'il puisse examiner si les prescriptions de protection des données sont respectées (voir art. 49, al. 3 et 50, al. 1, let. a, LPD).

3.8.5 **Question** : *L'exploitation d'un système de vidéosurveillance par un organe fédéral est-elle une activité de traitement qui doit figurer dans le registre des activités de traitement et doit être déclarée au PFPDT ?*

L'obligation de tenir un registre des activités de traitement au sens de l'art. 12 LPD concerne toutes les activités de traitement d'un responsable du traitement ou de son sous-traitant. Tant que des personnes sont identifiées ou identifiables sur l'enregistrement vidéo, alors la surveillance exercée par l'organe fédéral est soumise à la LPD et donc aux dispositions relatives à la tenue d'un registre des activités de traitement (les bases légales spéciales sont réservées). Cela signifie p. ex. que l'utilisation de caméras pour surveiller l'entrée d'un bâtiment de l'administration fédérale doit être signalée au PFPDT.

3.8.6 **Question** : *Y a-t-il des exceptions à l'obligation de tenir un registre des activités de traitement ?*

D'après l'art. 12, al. 5, LPD en rel. avec l'art. 24 OPDo, les entreprises et autres organismes de droit privé employant moins de 250 collaborateurs au 1er janvier d'une année (indépendamment de leur taux d'occupation) et les personnes physiques sont déliés de leur obligation de tenir un registre des activités de traitement. Cette exception ne vaut cependant pas si (a) le traitement porte sur des données sensibles (p. ex. données concernant la santé ; au sujet de ce terme, voir question 2.1.2) à grande échelle ou (b) si le traitement constitue un profilage à risque élevé (au sujet de ce terme, voir question 2.3.2). Ces entreprises devront tenir un registre des activités de traitement pour ces traitements de données précis (mais pas pour tous les autres traitements qu'elles effectuent).

Pour savoir quand l'on est en présence d'un traitement de données sensibles à grande échelle, voir le ch. 3.6.2.3.

Les personnes exemptées de cette obligation peuvent naturellement tenir un registre de leurs activités de traitement si elles le souhaitent. Il s'agit d'un instrument simple et efficace qui permet au responsable du traitement traitant régulièrement des données personnelles de garder une vue d'ensemble sur les activités de traitement. Cela peut aussi aider le responsable du traitement à respecter d'autres obligations, telles que le devoir d'information lors de la collecte de données personnelles (voir question 6.1.1).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6656 ; Rapport explicatif relatif à l'OPDo, p. 50.

4. Obligation des responsables du traitement privés ayant leur siège ou leur domicile à l'étranger de désigner un représentant

4.1 Conditions

4.1.1 **Question** : *Quels responsables du traitement étrangers doivent désigner un représentant en Suisse ?*

En application de l'art. 14, al. 1, LPD, certains responsables du traitement étrangers doivent désigner un représentant en Suisse. Cette obligation concerne les responsables du traitement privés ayant leur siège ou leur domicile à l'étranger et qui traitent des données personnelles concernant des personnes en Suisse (phrase introductive) et que ce traitement remplit (toutes) les conditions suivantes :

- Le traitement est en rapport avec *l'offre de biens ou de services* ou *le suivi du comportement de personnes en Suisse* (let. a) : c'est le cas par exemple lorsque le responsable du traitement exploite un commerce en ligne et que son offre est en francs suisses, ou qu'il prévoit la livraison en Suisse. En revanche, le simple fait qu'un site ou une adresse électronique soit accessible depuis la Suisse ne suffit pas à remplir cette condition. Le responsable procède au suivi du comportement de personnes en Suisse lorsqu'il observe les activités de ces personnes sur Internet. Cette condition vise en particulier les réseaux sociaux.
- Il s'agit d'un *traitement à grande échelle* (let. b ; à ce sujet, voir question 3.6.2.3).
- Le *traitement* est *régulier* (let. c) : cette condition devrait être remplie p. ex. dans le domaine du commerce en ligne. Lorsque les données personnelles constituent la « matière première » d'une activité (p. ex. pour les réseaux sociaux), il s'agit aussi d'un traitement régulier. En revanche, un traitement n'est pas régulier quand les données ne sont traitées que pendant une durée limitée ou de manière occasionnelle.
- Le traitement *présente un risque élevé pour la personnalité des personnes concernées* (let. d) : il faut examiner ce point au cas par cas. Le risque élevé peut notamment résulter de la quantité et du type de données traitées (s'il s'agit de données sensibles), le but du traitement, et la manière dont les données sont traitées (p. ex. utilisation de nouvelles technologies), d'une éventuelle communication des données à l'étranger et des droits d'accès aux données (p. ex. si un nombre important, voire illimité de personne peut accéder aux données).

Ce sont principalement les grandes plateformes et les réseaux sociaux ayant leur siège à l'étranger qui devront désigner un représentant en Suisse.

Conformément à l'art. 14, al. 3, LPD, les responsables du traitement étrangers doivent publier le nom et l'adresse de leur représentant. Ils peuvent par exemple le faire sur leur site web.

4.1.2 **Question** : *Que se passe-t-il si un responsable du traitement étranger ne désigne pas de représentant en Suisse ?*

Le PFPDT peut ordonner, dans une décision, au représentant étranger qui remplit les conditions énoncées à l'art. 14, al. 1, LPD, de désigner un représentant en Suisse (art. 51, al. 4, LPD). Puisqu'il s'agit d'un document officiel, la décision du PFPDT doit passer par la voie diplomatique (sauf si un accord international prévoit une notification directe). Au moment de la notification de sa décision, le PFPDT peut également menacer le responsable étranger d'une sanction en cas de non-respect de celle-ci (art. 63 LPD). Si une amende est prononcée en vertu de cette disposition, elle ne pourra être exécutée que par le biais de l'entraide judiciaire, ou il faudra également passer par la voie diplomatique pour la faire exécuter.

4.2 Tâches et obligations du représentant

Question : *Quelles sont les tâches et les obligations du représentant en Suisse ?*

Le représentant sert de point de contact en Suisse pour les personnes concernées et le PFPDT (art. 14, al. 2, LPD). Il a donc un rôle d'interlocuteur, mais il ne peut être tenu responsable d'éventuelles violations de la protection des données. En application de l'art. 15 LPD, trois obligations incombent au représentant :

- Il tient un registre des activités de traitement du responsable du traitement (al. 1) : ce registre doit contenir les informations décrites à l'art. 12, al. 2, LPD (voir question 3.8.3). Pour l'essentiel, il s'agit d'une description générale des activités de traitement. En principe, le registre ne contient pas de données personnelles.
- Il fournit sur demande au PFPDT les indications contenues dans ce registre (al. 2) : le PFPDT ne peut en revanche pas demander au représentant de lui fournir des informations ou des données personnelles provenant de l'étranger. S'il a besoin de ce type d'informations, le PFPDT doit passer par la voie de l'entraide judiciaire.
- Il fournit sur demande à la personne concernée des renseignements concernant l'exercice de ses droits (al. 3) : il peut s'agir de l'adresse du responsable du traitement ou des coordonnées de son conseiller à la protection des données. Même si le représentant fait office de point de contact pour les personnes concernées, le responsable du traitement reste celui qui est tenu de respecter le devoir d'information lors de la collecte de données personnelles (voir question 6.1.1). Les personnes concernées peuvent seulement faire valoir leur droit d'accès (voir question 7.2.1) auprès du responsable du traitement, mais pas de son représentant.

5. Communication de données personnelles à l'étranger

5.1 Généralités

Question : *Quand des données personnelles peuvent-elles être communiquées à l'étranger ?*

Conformément à l'art. 16, al. 1, LPD, des données personnelles peuvent être communiquées à l'étranger lorsque le Conseil fédéral a constaté que l'État concerné dispose d'une législation assurant un niveau de protection adéquat ou qu'un organisme international garantit un niveau de protection adéquat (voir ch. 5.2)

En l'absence d'une évaluation du Conseil fédéral, des données personnelles peuvent uniquement être communiquées à l'étranger dans les cas décrits à l'art. 16, al. 2 et 3 LPD (liste de

garanties permettant d'assurer un niveau de protection des données adéquat ; voir ch. 5.3) ou de l'art. 17 LPD (exceptions ; voir ch. 5.4)

Un niveau de protection approprié peut être garanti par :

- un traité international (art. 16, al. 2, let. a, LPD) ;
- les clauses de protection des données d'un contrat entre le responsable du traitement ou le sous-traitant et son cocontractant, préalablement communiquées au PFPDT (art. 16, al. 2, let. b, LPD) ;
- des garanties spécifiques élaborées par l'organe fédéral compétent et préalablement communiquées au PFPDT (art. 16, al. 2, let. c, LPD) ;
- des clauses types de protection des données préalablement approuvées, établies ou reconnues par le PFPDT (art. 16, al. 2, let. d, LPD) ;
- des règles d'entreprise contraignantes (« Binding Corporate Rules ») préalablement approuvées par le PFPDT ou par une autorité chargée de la protection des données relevant d'un État qui assure un niveau de protection adéquat (art. 16, al. 2, let. e, LPD) ;
- un code de conduite ou des certifications (art. 16, al. 3, LPD en rel. avec art. 12 OPDo).

Au sujet de la communication de données personnelles à l'étranger, voir également les informations et documents du PFPDT < https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html >

5.2 Evaluation de l'adéquation par le Conseil fédéral

5.2.1 **Question** : *Où trouver la liste des États et des organismes internationaux disposant d'un niveau de protection adéquat ?*

Conformément à la nouvelle LPD, c'est le Conseil fédéral, et non (plus) le PFPDT qui détermine quels États et organismes internationaux offrent un niveau de protection adéquat.

La liste des États, territoires, secteurs déterminés dans un État, et organismes internationaux avec un niveau de protection adéquat selon le Conseil fédéral figure à l'annexe 1 de l'OPDo et peut être consultée sur le site de l'Office fédéral de la justice : <https://www.bj.admin.ch/bj/fr/home/staat/datenschutz/internationales/anerkennung-staaten.html>.

5.2.2 **Question***: Sur quels critères le Conseil fédéral se base-t-il pour évaluer si un État ou un organisme international dispose d'un niveau de protection adéquat ?*

L'art. 8, al. 2, OPDo fixe plusieurs critères que le Conseil fédéral doit prendre en compte pour évaluer le niveau d'adéquation. Il s'agit notamment :

- des engagements internationaux de l'État ou de l'organisme international, notamment en matière de protection des données (let. a) ;
- de l'état de droit et du respect des droits de l'homme (let. b).
- de la législation applicable, notamment en matière de protection des données, de même que sa mise en œuvre et de la jurisprudence y relative (let. c) ;
- de la garantie effective des droits des personnes concernées et des voies de droit (let. d) ;
- du 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 (let. e).

Le PFPDT est consulté à chaque évaluation, et les appréciations effectuées par des organismes internationaux ou des autorités étrangères chargées de la protection des données peuvent être prises en compte (art. 8, al. 3, OPDo).

Le Conseil fédéral réévalue périodiquement l'adéquation du niveau de protection (art. 8, al. 4, OPDo). Les évaluations doivent être publiées (art. 8, al. 5, OPDo) et sont disponibles via le lien suivant : <https://www.bj.admin.ch/bj/fr/home/staat/datenschutz/internationales.html>.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6656 s. ; Rapport explicatif relatif à l'OPDo, p. 31.

5.3 Garanties d'un niveau de protection approprié

5.3.1 **Question** : *Quelles exigences s'appliquent aux clauses de protection des données d'un contrat (art. 16, al. 2, let. b, LPD) et aux garanties spécifiques (art. 16, al. 2, let. c, LPD) ?*

En l'absence d'une évaluation de l'adéquation par le Conseil fédéral (voir ch. 5.2), dans le secteur privé, le niveau de protection approprié peut être garanti par des *clauses de protection des données d'un contrat* entre le responsable du traitement ou le sous-traitant et son cocontractant (art. 16, al. 2, let. b, LPD). De la même manière, dans le secteur public, un organe fédéral compétent peut élaborer des *garanties spécifiques* (art. 16, al. 2, let. c, LPD).

Contrairement aux clauses type de protection des données (voir question 5.3.2), les clauses de protection contractuelles s'appliquent uniquement à la communication de données qui est prévue dans le contrat.

L'art. 9, al. 1, OPDo définit ce que les clauses de protection des données d'un contrat et les garanties spécifiques doivent régler au minimum. Il s'agit des éléments suivants :

- l'application des principes de licéité, de bonne foi, de proportionnalité, de transparence, de finalité et d'exactitude (let. a),
- les catégories de données communiquées et de personnes concernées (let. b),
- le type et la finalité de la communication des données personnelles (let. c),
- le cas échéant, le nom des États ou des organismes internationaux auxquels sont destinées les données personnelles, et les conditions applicables à la communication (let. d),
- les conditions applicables à la conservation, à l'effacement et à la destruction des données personnelles (let. e) ;
- les destinataires ou catégories de destinataires (let. f),
- les mesures visant à garantir la sécurité des données (let. g, voir les questions ch. 3.6)
- l'obligation d'annoncer les violations de la sécurité des données (let. h ; voir les questions ch. 6.4) ;
- si les destinataires sont des responsables du traitement, l'obligation pour le responsable du traitement destinataire d'informer les personnes concernées du traitement des données (let. i ; voir les questions ch. 6.1) ;
- les droits de la personne concernée, en particulier le droit d'accès et le droit à la remise ou à la transmission des données personnelles, le droit de s'opposer à la communication des données, le droit de demander la rectification, l'effacement ou la destruction de données et le droit de saisir en justice une autorité indépendante (let. j, voir les questions ch. 7).

Contrairement aux clauses type de protection des données (voir question 5.3.2) ou aux règles d'entreprise contraignantes (voir question 5.3.3), le PFPDT n'a pas besoin d'approuver les clauses de protection des données d'un contrat et les garanties spécifiques. Il suffit de les lui communiquer (préalablement à la communication des données à l'étranger) (art. 16, al. 2, let. b et c LPD et art. 9, al. 3, OPDo).

Le responsable du traitement et son sous-traitant (seulement dans le cas de clauses de protection des données d'un contrat) doivent prendre les mesures adéquates pour s'assurer que le destinataire respecte ces clauses ou garanties spécifiques (art. 9, al. 2, OPDo).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6658 s. ; Rapport explicatif relatif à l'OPDo, p. 34 ss.

5.3.2 **Question** : *À quelles exigences sont soumises les clauses type de protection des données (art. 16, al. 2, let. d, LPD) ?*

En l'absence d'une évaluation de l'adéquation par le Conseil fédéral (voir ch. 5.3), des *clauses type de protection des données* (art. 16, al. 2, let. d, LPD) peuvent garantir un niveau de protection approprié.

Les clauses type de protection des données peuvent être élaborées par des personnes privées, par les milieux intéressés ou par des organes fédéraux. Elles doivent préalablement avoir été approuvées par le PFPDT. Aucune donnée ne peut être communiquée à l'étranger avant que le PFPDT ait rendu sa décision au sujet des clauses types, à moins que la communication puisse se fonder sur d'autres garanties prévues à l'art. 16, al. 2, LPD (voir les questions 5.3.1 et 5.3.3) ou une dérogation au sens de l'art. 17 LPD (voir question 5.4). Le PFPDT communique le résultat de son examen dans un délai de 90 jours (art. 10, al. 2, OPDo).

Les clauses type de protection des données peuvent également être émises ou reconnues par le PFPDT lui-même. La liste de ces clauses est publiée sur le site web du PFPDT : https://www.edoeb.admin.ch/edoeb/fr/home/deredoeb/infothek/infothek-ds.html

Exemple : Le PFPDT a reconnu les clauses contractuelles types de la Commission européenne (Décision d'exécution [UE] 2021/914 du 4 juin 2023 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement [UE] 2016/679 du Parlement européen et du Conseil).

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, il doit prendre les mesures adéquates pour s'assurer que le destinataire les respecte (art. 10, al. 1, OPDo).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6659 s. ; Rapport explicatif relatif à l'OPDo, p. 35 s.

5.3.3 **Question** : *À quelles exigences sont soumises les règles d'entreprise contraignantes (art. 16, al. 2, let. e, LPD) ?*

En l'absence d'une évaluation de l'adéquation par le Conseil fédéral (voir ch. 5.2), la communication de données personnelles à une entreprise étrangère appartenant au même groupe (voir art. 11, al. 1, OPDo) peut être garantie par des *règles d'entreprise contraignantes* (« Binding corporate rules ») (art. 16, al. 2, let. e, LPD).

Les règles d'entreprise contraignantes doivent être préalablement approuvées par le PFPDT ou par une autorité chargée de la protection des données relevant d'un État qui assure un niveau de protection adéquat. Ce n'est qu'une fois ces règles approuvées que des données personnelles pourront être communiquées à l'étranger. Le PFPDT communique le résultat de son examen dans un délai de 90 jours (art. 11, al. 3, OPDo). Si les règles ont déjà été approuvées par une autorité chargée de la protection des données relevant d'un État qui assure un niveau de protection adéquat, il n'est pas nécessaire que le PFPDT se prononce également.

L'art. 11 OPDo précise les indications minimales que doivent contenir les règles d'entreprise contraignantes. Elles doivent au moins porter sur les mêmes points que les clauses de protection des données d'un contrat ou les garanties spécifiques mentionnés à l'art. 9, al. 1, OPDo (voir à ce sujet la question 5.3.1). Mais elles doivent également mentionner (art. 11, al. 2, OPDo) :

- la structure et les coordonnées du groupe d'entreprises et de chacune de ses entités, et
- les mesures mises en place au sein des groupes d'entreprises pour garantir le respect des règles d'entreprise contraignantes.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6660 s. ; Rapport explicatif relatif à l'OPDo, p. 36.

5.3.4 **Question** : *Existe-t-il d'autres garanties pour assurer un niveau de protection approprié et permettre de communiquer des données à l'étranger ?*

Oui. Conformément à l'art. 16, al. 3, LPD en rel. avec l'art. 12, al. 1, OPDo, des données personnelles peuvent être communiquées à l'étranger lorsqu'un code de conduite ou une certification garantit un niveau de protection approprié. Le code de conduite doit être préalablement soumis au PFPDT pour approbation (art. 12, al. 2, OPDo). Le code de conduite ou la certification doivent être assortis 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 cet instrument (art. 12, al. 3, OPDo).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6660 ; Rapport explicatif relatif à l'OPDo, p. 36.

5.4 Dérogations

Question : *Des données peuvent-elles être exceptionnellement communiquées à l'étranger en l'absence d'une évaluation de l'adéquation par le Conseil fédéral ou sans qu'un niveau de protection approprié des données ne soit garanti ?*

Oui. D'après l'art. 17, al. 1, LPD, des données personnelles peuvent *exceptionnellement* être communiquées à l'étranger en l'absence d'une évaluation de l'adéquation (voir ch. 5.2) ou sans garantie d'un niveau de protection approprié des données (voir ch. 5.3), dans les cas suivants :

- La personne concernée a expressément donné son consentement à la communication (let. a).
- La communication est en relation directe avec la conclusion et l'exécution d'un contrat entre le responsable du traitement et la personne concernée ou entre le responsable du traitement et son cocontractant, dans l'intérêt de la personne concernée (let. b). Dans ce cas, le PFPDT devra, s'il le demande, être informé des communications de données (art. 17, al. 2, OPDo).

- la communication est nécessaire à la sauvegarde d'un intérêt public prépondérant, ou à la constatation, à l'exercice ou à la défense d'un droit devant un tribunal ou une autre autorité étrangère compétente (let. c). Sur demande, le PFPDT devra également être informé (art. 17, al. 2, OPDo).
- la communication est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable (let. d). Le PFPDT doit être informé sur demande (art. 17, al. 2, OPDo).
- la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement (let. e).
- les données personnelles proviennent d'un registre prévu par la loi, accessible au public ou à toute personne justifiant d'un intérêt légitime, pour autant que les conditions légales pour la consultation dans le cas d'espèce soient remplies (let. f).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6661 s.

6. Obligations du responsable du traitement et du sous-traitant

6.1 Devoir d'informer du responsable lors de la collecte de données personnelles

6.1.1 **Question** : *Qu'est-ce que le devoir d'informer lors de la collecte de données personnelles ?*

Conformément à l'art. 19, al. 1, LPD, le responsable du traitement doit informer la personne concernée de manière adéquate lors de la collecte de données personnelles. Il s'agit de l'un des principes centraux du droit de la protection des données. C'est seulement lorsqu'une personne sait que des données qui la concernent sont traitées qu'elle peut décider comment agir.

La révision totale de la LPD a étendu ce devoir d'informer à tous les types de données personnelles (art. 19, al. 1, LPD). Cette obligation n'est pas nouvelle pour les organes fédéraux, mais le changement concerne avant tout les responsables du traitement privés, qui devaient uniquement informer lors de la collecte de données personnelles sensibles ou de profils de la personnalité en vertu de l'ancien droit. Cela permet de renforcer la transparence des traitements de données ainsi que l'autodétermination informationnelle de la population.

Comme par le passé, le devoir d'informer s'applique même lorsque les données personnelles ne sont pas directement collectées auprès de la personne concernée, mais par le biais de tiers (art. 19, al. 1, 2e partie de la phrase, LPD).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6668 s.

6.1.2 **Question** : *Y a-t-il des exceptions au devoir d'informer lors de la collecte de données personnelles ?*

Oui. L'art. 20 LPD prévoit des exceptions au devoir d'informer (al. 1 et 2) et la possibilité de restreindre des communications après une pesée des intérêts (al. 3 et 4).

Il y a une *exception* au devoir d'information, lorsque :

- la personne concernée dispose déjà des informations correspondantes (art. 20, al. 1, let. a, LPD) ;

  Exemple : La personne concernée a déjà donné son consentement au traitement des données.

- le traitement des données personnelles est prévu par la loi (art. 20, al. 1, let. b, LPD) ;

  Cette exception peut concerner aussi bien les traitements effectués par des organes fédéraux que par des responsables du traitement privés. Dans ce cas, la personne concernée doit pouvoir reconnaître les éléments clés du traitement de données dans la base légale.

- les données personnelles ne sont pas collectées auprès de la personne concernée et que l'information au sujet du traitement est impossible à donner ou qu'elle nécessite des efforts disproportionnés (art. 20, al. 2, LPD).

Le responsable du traitement peut restreindre ou différer la communication des informations, ou y renoncer, lorsque :

- les intérêts prépondérants d'un tiers l'exigent (art. 20, al. 3, let. a, LPD) ;
- le responsable du traitement est une personne privée, que ses intérêts prépondérants l'exigent, et qu'il ne communique pas les données à un tiers (n'appartenant pas au même groupe d'entreprises, voir art. 20, al. 4, LPD) (art. 20, al. 3, let. c, LPD) ;
- le responsable du traitement est un organe fédéral et que l'intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Suisse, l'exige (art. 20, al. 3, let. d, LPD).

L'information ne doit pas être limitée au-delà de ce qui est absolument nécessaire et son motif doit être mis en relation avec l'intérêt à la transparence du traitement. De manière générale, il faut choisir la solution la plus favorable à la personne concernée afin de garantir autant que possible la transparence du traitement compte tenu des circonstances.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6672 s.

6.1.3 **Question** : *Quelles informations le responsable du traitement doit-il communiquer à la personne concernée ?*

Conformément à l'art. 19, al. 2, phrase introductive, LPD, les personnes concernées doivent disposer de toutes les informations nécessaires pour faire valoir leurs droits selon la LPD et pour que la transparence des traitements soit garantie. Cette disposition permet de mettre en œuvre le devoir d'informer de façon souple et adaptée aux risques. Le responsable du traitement doit fournir des informations plus ou moins détaillées en fonction du type de données traitées, de la nature et de la portée du traitement en question.

Les informations devant être fournies au minimum sont les suivantes : l'identité (le nom ou l'entreprise) et les coordonnées du responsable du traitement (art. 19, al. 2, let. a, LPD), la finalité du traitement (art. 19, al. 2, let. b, LPD) et, le cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises (art. 19, al. 2, let. c). Dans cette disposition, les sous-traitants font également partie des destinataires. Le responsable du traitement doit donc également informer les personnes concernées, lors de la collecte de données, que leurs données peuvent être communiquées à un sous-traitant. S'il ne collecte pas directement les données personnelles auprès de la personne concernée, mais auprès de tiers, il doit en outre communiquer les catégories de données traitées à cette dernière (art. 19, al. 3, LPD). Lorsque des données personnelles sont communiquées à l'étranger, le responsable du traitement lui indique également le nom de l'État ou de l'organisme international auquel elles sont communiquées et, le cas échéant, les garanties prévues à l'art. 16, al. 2 LPD (à ce sujet, voir les questions du ch. 5.3), ou l'application d'une des exceptions prévues à l'art. 17 LPD (à ce sujet, voir les questions du ch. 5.4) (art. 19, al. 4, LPD).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6669 s.

6.1.4 **Question** : *De quelle façon la personne concernée doit-elle être informée de la collecte de ses données personnelles ? Est-ce que la publication des informations nécessaires sur un site web est suffisante ?*

La LPD ne règle pas exactement de quelle manière il faut informer la personne concernée. L'art. 19, al. 1, LPD mentionne seulement que l'information doit se faire « de manière adéquate ». C'est l'art. 13 OPDo qui dispose concrètement que le responsable du traitement doit communiquer aux personnes concernées les informations sur la collecte de données personnelles de manière concise, transparente, compréhensible et facilement accessible.

Ni la loi ni l'ordonnance ne fixent de règles quant à la forme de l'information. Il peut donc par exemple s'agir d'une déclaration de confidentialité, de conditions générales de vente, d'un courrier séparé, ou des pictogrammes. Le responsable du traitement doit garantir que les personnes concernées puissent prendre effectivement connaissance de l'information, en particulier quand les données personnelles ne sont pas collectées auprès d'elles. Dans ce cas, il est possible que le simple fait de mettre à disposition les informations sur un site ne suffise pas. La personne concernée doit savoir, et il faut donc l'en informer activement, que ces informations se trouvent sur un site en particulier.

Dans le cas d'un entretien téléphonique, des explications orales peuvent également être fournies, lesquelles peuvent être complétées par une référence vers un site web ; s'il s'agit d'informations enregistrées, la personne concernée devra avoir la possibilité d'entendre des informations plus détaillées. Enfin, dans le cas où la personne est filmée par un système de vidéosurveillance fixe ou par un drone, un panneau indicateur ou une campagne d'information devront par exemple mentionner cette activité.

Le responsable du traitement doit s'assurer, lors du choix des modalités d'informations, que les informations les plus importantes sont toujours transmises dans le premier niveau de communication avec la personne concernée lors de la collecte de ses données personnelles. Par exemple, lorsque la communication se fait sur un site Internet, une bonne pratique peut consister à faire en sorte que les informations essentielles soient toutes disponibles en un coup d'œil, par exemple sous la forme d'un aperçu. Pour obtenir des informations complémentaires, la personne pourra ensuite cliquer sur ces premières informations, et ouvrir une autre fenêtre contenant des détails supplémentaires.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6668 s. ; Rapport explicatif relatif à l'OPDo, p. 37.

6.2 Décision individuelle automatisée

6.2.1 **Question***: Qu'est-ce qu'une décision individuelle automatisée ?*

Une décision automatisée est une décision prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour la personne concernée ou l'affecte de manière significative (art. 21, al. 1, LPD). Définition détaillée :

- *Automatisation complète :* En cas de décision individuelle automatisée, l'appréciation de la teneur des faits et la décision qui en découle sont issues d'une machine ou d'un algorithme, sans l'intervention d'un humain. Il est toutefois indifférent que la programmation de cet algorithme ait été assurée par un humain ou non. On est aussi en présence d'une décision individuelle automatisée lorsque celle-ci est communiquée par une personne physique, qui ne l'a cependant pas prise elle-même ou qui a uniquement vérifié des aspects formels.

En revanche, il n'y a pas de décision individuelle automatisée lorsque seule la préparation de la décision est automatisée, mais qu'elle est ensuite prise par un humain.

- *Complexité* : Une décision individuelle automatisée doit également présenter un certain degré de complexité. Toutefois, l'objectif de protection ressortant des dispositions ad hoc (notamment les art. 21, 25, al. 2, let. f et 34, al. 2, let. c, LPD) permet de conclure qu'il est question spécialement des processus de décision qui ne sont pas intelligibles pour les personnes concernées. Dans le sens d'une interprétation téléologique de l'art. 21, al. 1, LPD, il ne faudrait pas inclure dans la notion de décision individuelle automatisée les décisions triviales du type « si…donc » ou les interrogations « oui/non » concernant des critères objectifs et qui sont aisément compréhensibles pour la personne concernée.

  Exemples : il n'y a pas de décision individuelle automatisée au sens de l'art. 21, al. 1, LPD lors d'un retrait d'argent d'un avoir existant à un bancomat ou lors d'un contrôle de l'accès par carte à puce, sur la base d'une liste prédéfinie de personnes admises. Des opérations mathématiques simples (comme l'addition de valeurs) ne devraient pas non plus être considérées comme étant d'un degré de complexité tel qu'elles constituent des décisions individuelles automatisées.

- *Effet* : Seules les décisions ayant des *effets juridiques* pour la personne concernée, ou qui l'affectent de manière significative sont considérées comme des décisions individuelles automatisées au sens de l'art. 21, al. 1, LPD.

  Une décision produit des effets juridiques si elle a des conséquences directes et prévues par la loi pour la personne concernée. Dans le domaine du droit privé, c'est le cas notamment pour la conclusion ou la dénonciation d'un contrat. En règle générale, il n'y a pas d'effets juridiques si un contrat n'est pas signé (il y a toutefois une situation particulière dans le domaine des obligations de contracter). Un contrat non conclu peut toutefois affecter l'intéressé de manière significative. Dans le domaine du droit public, il y a des effets juridiques notamment lorsqu'une décision est prise de manière entièrement automatisée.

  Il y a lieu de supposer que la personne concernée est affectée *de manière significative* si elle subit des restrictions durables, par exemple de ses intérêts économiques ou personnels. De simples inconvénients ne sont pas suffisants. Tout dépend des circonstances concrètes du cas particulier. Il convient de tenir compte notamment de l'importance que le bien en question revêt pour la personne concernée, de la durabilité de l'effet de la décision, et il faut examiner si des alternatives sont possibles. S'il s'agit d'un bien de première importance, il faut s'assurer de l'existence de réelles alternatives (p. ex. logement ou place de travail).

  Exemple : Une personne peut être affectée de manière significative si des prestations médicales sont attribuées sur la base de décisions automatisées.

Il faut distinguer la décision individuelle automatisée du profilage, même si ces deux procédés peuvent se recouper. Le traitement de données à la base d'une décision individuelle automatisée peut être un profilage, mais il ne l'est pas forcément. Inversement, un profilage peut aboutir à une décision individuelle automatisée, mais pas impérativement (p. ex. si le profilage sert uniquement à l'examen préalable, en vue d'une décision qui sera prise par un humain). La suppression de la mention « y compris le profilage » par le Parlement à l'art. 19, al. 1 du projet du Conseil fédéral de révision totale de la LPD n'a pas de conséquences sur le plan matériel (comme l'avait expliqué la cheffe du DFJP au Conseil des États le 18 décembre 2019). Le profilage n'avait pas d'implications distinctes dans cette disposition. Il entre en effet dans le champ d'application de l'art. 21, al. 1, LPD, qu'il soit mentionné ou non tant qu'il donne lieu à une décision individuelle automatisée.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6673 ss ; Note de l'OFJ sur la révision totale de la LPD, p. 19 ss ; BO 2019 N 1241 (intervention de la cheffe du DFJP lors de l'examen de la révision totale dee la LPD au Conseil des États du 18 décembre 2019)

6.2.2 **Question** : *Quels sont les droits de la personne concernée en cas de décision individuelle automatisée ?*

Le nouveau droit de la protection des données prévoit que la personne concernée doit être informée en cas de décision individuelle automatisée (art. 21, al. 1, LPD). Si cette décision émane d'un organe fédéral, ce dernier doit la qualifier comme telle (art. 21, al. 4, 1re phrase, LPD). Par ailleurs, la personne concernée a le droit de demander qu'on lui donne la possibilité de faire valoir son point de vue et d'exiger que la décision individuelle automatisée soit revue par une personne physique (art. 21, al. 2, LPD).

L'obligation du responsable du traitement d'informer et le droit de la personne concernée d'être entendue ne s'appliquent pas, conformément à l'art. 21, al. 3, LPD, lorsque la décision individuelle automatisée est en relation directe avec la conclusion et l'exécution d'un contrat entre le responsable du traitement et la personne concernée et que la demande de cette dernière est satisfaite (let. a), ou lorsque la personne concernée a expressément consenti à ce que la décision soit prise de manière automatisée (let. b, au sujet des critères du consentement, voir question 3.4.2). L'art. 21, al. 2, LPD n'est pas applicable aux organes fédéraux lorsqu'ils ne sont pas tenus d'entendre la personne concernée avant la décision conformément à l'art. 30, al. 2 de la loi fédérale 8 sur la procédure administrative (PA ; RS 172.021) ou en vertu d'une autre loi fédérale (p. ex. quand une décision individuelle automatisée peut être revue dans le cadre d'une procédure de recours non automatisée). De cette façon, la LPD est coordonnée avec le droit de la procédure administrative.

Enfin, la personne concernée doit obtenir, dans le cadre de son droit d'accès selon l'art. 25, al. 2, let. f, LPD, des informations sur l'existence d'une décision individuelle automatisée ainsi que sur la logique sur laquelle se base la décision (au sujet du droit d'accès, voir les questions ch. 7.2).

Référence : À propos des exigences posées pour les bases légales permettant aux organes fédéraux de procéder à des décisions individuelles automatisées, voir la Note de l'OFJ sur la révision totale de la LPD, p. 22.

6.3 Analyse d'impact relative à la protection des données personnelles

6.3.1 **Question** : *Qu'est-ce qu'une analyse d'impact relative à la protection des données personnelles ?*

Celui qui envisage un traitement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée doit procéder au préalable à une analyse d'impact relative à la protection des données personnelles (art. 22, al. 1, LPD). L'analyse d'impact est un instrument d'évaluation des risques. Elle doit contenir une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, ainsi que les mesures prévues pour protéger sa personnalité et ses droits fondamentaux (art. 22, al. 3, LPD). L'avantage pour le responsable du traitement est qu'elle permet d'anticiper d'éventuels problèmes en matière de protection des données.

Le responsable du traitement doit conserver l'analyse d'impact relative à la protection des données personnelles pendant au moins deux ans après la fin du traitement (art. 14 OPDo).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6676 s. ; Rapport explicatif relatif à l'OPDo, p. 37 s.

6.3.2 **Question** : *Quand faut-il faire une analyse d'impact relative à la protection des données personnelles ?*

Il faut procéder à une analyse d'impact relative à la protection des données personnelles lorsque le traitement prévu peut entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 22, al. 1, LPD). L'existence d'un risque élevé doit être évaluée selon différents facteurs de risque. Selon l'art. 22, al. 2, LPD, l'existence d'un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. À titre d'exemple, la LPD cite deux cas dans lesquels le risque est élevé : lors du traitement de données sensibles à grande échelle (voir question 3.6.2.3) et en cas de surveillance systématique de grandes parties du domaine public (art. 22, al. 2, let. a et b, LPD).

Les responsables du traitement privés sont *déliés* de l'obligation d'établir une analyse d'impact s'ils sont tenus d'effectuer le traitement en vertu d'une obligation légale (art. 22, al. 4, LPD). Dans ce cas, on peut partir du principe que le législateur a déjà évalué les risques éventuels pour la personne concernée et édicté, le cas échéant, des prescriptions de protection pour y faire face.

Par ailleurs, le responsable du traitement privé peut renoncer à établir une analyse d'impact lorsqu'il recourt à un système, un produit ou un service certifié conformément à l'art. 13 LPD pour l'utilisation prévue ou qu'il respecte un code de conduite au sens de l'art. 11 LPD qui remplit différentes conditions (art. 22, al. 5, LPD).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6676 ss.

Documentation concernant l'analyse d'impact relative à la protection des données personnelles (AIPD) pour les organes fédéraux :

- Directives du Conseil fédéral concernant l'examen préalable des risques et l'analyse d'impact relative à la protection des données personnelles en cas de traitement de données personnelles par l'administration fédérale (FF 2023 1882)
- Instrument d'examen préalable des risques
- Guide AIPD

6.3.3 **Question** : *Quand faut-il consulter le PFPDT ?*

Lorsque l'analyse d'impact à 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 de la personne concernée, le responsable du traitement doit en principe consulter le PFPDT (art. 23, al. 1, LPD). Autrement dit, ce n'est que dans le cas où le responsable du traitement ne parvient pas à faire face de manière satisfaisante aux risques qu'il doit consulter le PFPDT.

Lorsque le PFPDT est consulté, il communique au responsable du traitement ses objections concernant le traitement envisagé dans un délai de deux mois. Ce délai peut être prolongé d'un mois lorsqu'il s'agit d'un traitement de données complexe (art. 23, al. 2, LPD). Si le PFPDT a des objections concernant le traitement envisagé, il propose au responsable du traitement des mesures appropriées (art. 23, al. 3, LPD).

Un responsable du traitement privé peut *renoncer* à consulter le PFPDT, s'il a consulté son conseiller à la protection des données au sens de l'art. 10 LPD (voir à ce sujet les questions 3.7.1 et 3.7.3).

6.4 Annonce des violations de la sécurité des données

6.4.1 **Question** : *Qu'est-ce qu'une violation de la sécurité des données ?*

À ce sujet, voir question 3.6.1.1.

6.4.2 **Question** : *Toutes les violations de la sécurité des données doivent-elles être annoncées au PFPDT ?*

Non, conformément à l'art. 24, al. 1, LPD, il faut seulement annoncer une violation de la sécurité des données au PFPDT si elle entraîne vraisemblablement un *risque élevé* pour la personnalité ou les droits fondamentaux de la personne concernée. Le responsable du traitement doit évaluer les conséquences possibles de la violation pour la personne concernée. Seules les violations de la sécurité des données doivent être annoncées, mais pas les cyberattaques qui ont été contrées ou qui n'ont pas fonctionné. Le responsable peut en revanche annoncer volontairement une violation de la sécurité des données dont il n'estime pas le risque élevé.

L'annonce au PFPDT se fait sur un portail prévu à cet effet (le « databreach-portal » : <https://databreach.edoeb.admin.ch/report>). Le responsable du traitement peut également l'annoncer sous une autre forme.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6680 ss.

6.4.3 **Question** : *Quelles informations doivent être fournies au PFPDT ?*

L'art. 24, al. 2, LPD spécifie les indications minimales que le responsable du traitement doit communiquer au PFPDT lors de l'annonce d'une violation de la sécurité des données : il s'agit de la nature de cette violation, de ses conséquences et des mesures prises ou envisagées. L'art. 15, al. 1, OPDo précise plus en détail le contenu de cette annonce. Outre les informations minimales prévues dans la loi, il faut communiquer, dans la mesure du possible, le moment et la durée de la violation, les catégories et le nombre approximatif de données personnelles concernées (p. ex. adresses, informations relatives aux cartes de crédit, données médicales). Ces informations sont importantes afin que le PFPDT puisse estimer la gravité de la violation. Par ailleurs, le responsable du traitement doit fournir le nom et les coordonnées d'une personne de contact pour la communication avec le PFPDT, et le cas échéant, la personne concernée (à ce sujet, voir question 6.4.5).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6681 ; Rapport explicatif relatif à l'OPDo, p. 38 s.

6.4.4 **Question** : *L'art. 24, al. 1, LPD dispose que les violations de la sécurité des données doivent être annoncées au PFPDT « dans les meilleurs délais » ? Qu'est-ce que cela signifie ?*

L'annonce doit avoir lieu dans les meilleurs délais à partir du moment où le traitement non autorisé est connu. Le responsable du traitement doit agir rapidement, mais la disposition lui laisse une certaine marge d'appréciation, qui dépend en pratique de l'ampleur du risque pour la personne concernée. Plus ce risque est élevé et le nombre de personnes concernées important, plus il doit informer rapidement le PFPDT.

L'art. 15, al. 2, OPDo permet au responsable du traitement de fournir progressivement les informations au PFPDT s'il n'est pas en mesure de fournir toutes les informations au moment où la violation de la sécurité des données est détectée. Dans un premier temps, il a le droit de ne fournir que les informations dont il dispose. Pour l'annonce des autres informations, la règle de l'art. 24, al. 1, LPD s'applique : le responsable doit faire l'annonce « dans les meilleurs délais » (question 6.4.4).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6681 ; Rapport explicatif relatif à l'OPDo, p. 38 s.

6.4.5 **Question** : *Dans quels cas faut-il informer la personne concernée d'une violation de la sécurité des données ?*

Le responsable du traitement doit informer la personne concernée lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige (art. 24, al. 4, LPD). La marge d'appréciation est assez large. Il faut se demander si l'information peut réduire les risques pour la personnalité ou les droits fondamentaux de la personne concernée, en lui permettant par exemple de prendre les dispositions nécessaires pour se protéger, comme modifier des données d'accès ou un mot de passe.

L'art. 15, al. 3, OPDo fixe les informations qui doivent être fournies à la personne concernée. Celles-ci doivent être communiquées dans un langage simple et compréhensible.

Dans certains cas, le responsable du traitement peut restreindre l'information de la personne concernée, la différer ou y renoncer, par exemple si un devoir légal de garder le secret l'interdit ou qu'il n'est pas possible de respecter le devoir d'information, ou encore que l'information nécessiterait des efforts disproportionnés. Ces exceptions figurent à l'art. 24, al. 5, LPD.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6681 s. ; Rapport explicatif relatif à l'OPDo, p. 38 s.

7. Droits de la personne concernée

7.1 Généralités

Question : *Quels sont les droits des personnes dont les données personnelles sont traitées ?*

La nouvelle la LPD améliore la transparence des traitements de données personnelles. Il s'agit d'un élément central du renforcement des droits de la personne concernée. En effet, ce n'est que lorsqu'une personne sait que ses données personnelles sont traitées qu'elle peut faire valoir ses droits en matière de protection des données. Outre le devoir du responsable du traitement d'informer lors de la collecte des données personnelles (art. 19 s. LPD ; voir les questions ch. 6.1), le droit d'accès de la personne concernée joue également un rôle fondamental (art. 25 ss LPD ; voir à ce sujet la question 7.2). Les personnes concernées peuvent demander au responsable des informations importantes relatives au traitement de leurs données personnelles. La LPD prévoit désormais également un droit à la remise ou à la transmission des données personnelles (art. 28 s. LPD ; voir à ce sujet la question 7.3)

Par ailleurs, les personnes concernées peuvent faire valoir certaines prétentions leur permettant d'influencer le traitement de leurs données. Elles ont par exemple le droit de s'opposer entièrement ou en partie à un traitement de données ou à la communication de leurs données personnelles (art. 30, al. 2, let. b en rel. avec art. 32, al. 2 et 37 LPD), de faire rectifier des

données personnelles inexactes (art. 32, al. 1 et 41, al. 2, let. a, LPD) et de faire effacer ou détruire des données traitées illicitement (art. 32, al. 2, let. c et 41, al. 2, let. a, LPD).

Pour faire valoir leurs droits, les personnes concernées peuvent s'adresser à des tribunaux indépendants et lancer une procédure civile ou administrative (art. 32 et 41 LPD). Par ailleurs, elles peuvent dénoncer une violation des prescriptions de protection des données auprès du PFPDT (art. 49, al. 1, LPD). Elles ne peuvent toutefois pas avoir la qualité de partie lors de l'enquête du PFPDT (art. 52, al. 2, LPD, a contrario). Le PFPDT doit en revanche les informer des démarches entreprises sur la base de leur dénonciation et du résultat de l'éventuelle enquête (art. 49, al. 4, LPD). Enfin, les personnes concernées peuvent déposer plainte auprès des autorités de poursuite pénale, par exemple en cas de violation des obligations d'informer ou de renseigner (art. 60 ss LPD ; voir à ce sujet les questions ch. 11)

7.2 Droit d'accès

7.2.1 **Question** : *Qu'est-ce que le droit d'accès ?*

Conformément à l'art. 25, al. 1, LPD, toute personne peut demander au responsable du traitement si des données personnelles la concernant sont traitées. Ce droit d'accès a été étendu lors de la révision totale de la LPD. La personne concernée doit recevoir les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la LPD et pour que la transparence du traitement soit garantie (art. 25, al. 2, phrase introductive, LPD). Le droit d'accès permet à la personne concernée de contrôler le traitement de ses données et de s'opposer à un éventuel traitement illicite (voir question 7.1).

L'art. 25, al. 2, LPD dresse une liste non exhaustive des informations qui doivent toujours être communiquées à la personne concernée : il s'agit d'abord de l'identité et des coordonnées du responsable du traitement, des données personnelles traitées en tant que telles et de la finalité du traitement (let. a à c). De plus, il faut lui indiquer la durée de conservation des données personnelles ou, si cela n'est pas possible, les critères pour fixer cette dernière (let. d). La personne concernée doit également obtenir les informations disponibles sur l'origine des données personnelles, dans la mesure où ces données n'ont pas été collectées auprès d'elle (let. e). Le cas échéant, il faudra lui indiquer l'existence d'une décision individuelle automatisée (voir les questions 6.2.1 et 6.2.2) ainsi que la logique sur laquelle se base la décision (let. f). Elle devra également pouvoir connaître les destinataires ou les catégories de destinataires auxquels ses données ont éventuellement été communiquées. Si les destinataires se trouvent à l'étranger, la personne concernée devra être informée de l'État concerné et des garanties qu'il prévoit, ou de l'application d'exceptions (let. g, voir à ce sujet le ch. 5)

Remarque : Un formulaire type et d'autres informations relatives à la procédure à suivre en cas de demande de renseignements sont disponibles sur le site du PFPDT :
<*https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/grundlagen/auskunftsrecht.html*>

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6683 s. ; Rapport explicatif relatif à l'OPDo, p. 40 ss.

7.2.2 **Question** : *Le droit d'accès peut-il être restreint ?*

Dans certains cas, le responsable du traitement peut refuser, restreindre ou différer la communication de renseignements (art. 26 et 27 LPD). Ces restrictions peuvent se justifier par un intérêt prépondérant privé ou public. Elles correspondent en grande partie à ce qui était déjà prévu auparavant.

Le responsable du traitement peut désormais également refuser, restreindre ou différer la communication de renseignements quand la demande d'accès est manifestement infondée ou procédurière (art. 26, al. 1, let. c, LPD). Cette exception doit être interprétée de manière restrictive. Le droit d'accès doit pouvoir être exercé inconditionnellement et sans la preuve d'un intérêt. Dans un arrêt principal sur l'exercice du droit d'accès contraire à la protection des données, le Tribunal fédéral admet toutefois que la motivation de la demande d'accès peut exceptionnellement être prise en compte lorsque le droit d'accès est exercé de façon abusive (dans un but étranger à la protection des données) (ATF 138 III 425, consid. 5.5). Selon le Tribunal fédéral, il y a par exemple abus de droit lorsque le demandeur utilise le droit d'accès uniquement pour espionner une (future) partie adverse et se procurer des preuves normalement inaccessibles ou pour économiser les frais qu'il devrait normalement payer pour obtenir ces données. Lorsqu'un renseignement n'est demandé que pour nuire au débiteur du droit d'accès, il considère également que l'exercice du droit d'accès est frauduleux. Au vu de l'importance cruciale du droit d'accès pour les droits de la personnalité et les droits fondamentaux des personnes concernées (voir question 7.2.1), il doit toujours être manifeste que le droit d'accès a été invoqué dans un but qui ne relève aucunement du champ d'application de la LPD.

Le responsable du traitement doit justifier pourquoi il refuse, restreint ou diffère le droit d'accès (art. 26, al. 4, LPD). Les explications doivent permettre à la personne concernée de vérifier si la restriction de son droit d'accès est justifiée.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6685 s. ; Rapport explicatif relatif à l'OPDo, p. 40 ss., ATF 138 III 425.

7.3 Droit à la remise ou à la transmission des données personnelles

Question : *Qu'est-ce que le droit à la remise ou à la transmission des données personnelles ?*

Conformément à l'art. 28 LPD, la personne concernée a la possibilité de demander au responsable du traitement de lui remettre sous un format électronique couramment utilisé les données personnelles la concernant qu'elle lui a communiquées, ou de les faire transmettre à un autre responsable du traitement. Les conditions requises sont que le responsable du traitement traite les données de manière automatisée (voir question 2.2.2), avec le consentement de la personne concernée ou en relation directe avec la conclusion ou l'exécution d'un contrat entre elle et lui. Si les données doivent être transmises à un autre responsable du traitement, il ne faut pas que cela exige des efforts disproportionnés (art. 28, al. 2, LPD).

Toujours selon l'art. 28 LPD, les données personnelles demandées peuvent être utilisées à différentes fins : pour un usage strictement personnel (p. ex. pour les enregistrer sur un espace de stockage) ou pour les transmettre à d'autres fournisseurs de services en ligne. Ce nouveau droit à la remise ou à la transmission des données personnelles vise à renforcer le contrôle que peut avoir la personne concernée sur ses données personnelles et leur réutilisation. Il facilite le passage entre différentes offres de services, ce qui favorise la concurrence et l'innovation.

L'art. 29 LPD règle les restrictions du droit à la remise ou à la transmission des données personnelles. Il repose largement sur les mêmes critères que ceux applicables au droit d'accès (voir question 7.2.2).

Référence : Pour plus d'informations sur le droit à la remise ou à la transmission des données personnelles, voir le Rapport explicatif relatif à l'OPDo, p. 43 ss.

8. Dispositions particulières pour le traitement de données personnelles par des personnes privées

Question : *Les responsables du traitement privés ont-ils besoin d'un motif justificatif pour traiter des données personnelles ?*

En Suisse, le traitement de données personnelles par des personnes privées (notamment des entreprises ou des personnes physiques) est en principe admis. Il ne doit être justifié que s'il porte, dans un cas d'espèce, atteinte à la personnalité de la personne concernée. En l'absence de motif justificatif, il est considéré comme illicite (art. 30, al. 1, et 31, al. 1, LPD). La LPD reprend ainsi le même principe que celui qui s'applique déjà, de façon générale, à la protection de la personnalité en vertu du code civil (art. 28 ss CC ; RS 210).

Tout traitement de données personnelles ne constitue pas une atteinte à la personnalité. C'est le cas uniquement si le traitement en question entraîne une atteinte d'une certaine gravité. L'art. 30, al. 2, LPD fournit une liste non exhaustive d'actes qui constituent une atteinte à la personnalité. Parmi eux figure le fait de :

- traiter des données personnelles en violation des principes définis aux art. 6 et 8 LDP (art. 30, al. 2, let. a, LPD ; c'est le cas, p. ex. lorsque des données personnelles sont traitées plus longtemps que nécessaire ou dans un but contraire à celui pour lequel elles ont été obtenues) ;
- traiter des données personnelles contre la manifestation expresse de la volonté de la personne concernée (art. 30, al. 2, let. b, LPD) ; ou
- communiquer à des tiers des données sensibles (art. 30, al. 2, let. c, LPD).

En règle générale, il n'y a cependant pas atteinte à la personnalité lorsque la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement (art. 30, al. 3, LPD).

Le fait qu'une atteinte à la personnalité soit établie ne signifie pas pour autant que le traitement des données est interdit. L'atteinte à la personnalité n'est illicite que si le traitement de données n'est pas justifié par un motif suffisant (art. 31, al. 1, LPD). Les trois motifs suivants peuvent ainsi être invoqués :

- *base légale* pour le traitement des données ;
- *intérêt privé ou public prépondérant au traitement des données* : ce motif nécessite une pesée des intérêts. L'art. 31, al. 2, LPD donne une liste non exhaustive des cas dans lesquels l'intérêt prépondérant du responsable du traitement entre en considération.
- *consentement* : lorsque le consentement de la personne concernée est utilisé comme motif justificatif à un traitement de données qui porte atteinte à sa personnalité, il doit satisfaire aux exigences de l'art. 6, al. 6 et 7, LPD (voir question 3.4.2).

Si l'atteinte à la personnalité ne peut pas être justifiée, la personne concernée peut faire valoir des prétentions de droit civil. À cet égard, l'art. 32, al. 2, LPD renvoie, comme c'était le cas sous l'ancien droit, aux actions prévues aux art. 28 ss CC. La personne concernée dispose ainsi des mêmes droits que pour les autres atteintes à la personnalité. Par souci de clarté, la LPD mentionne en outre expressément des droits spécifiques. Selon l'art. 32, al. 2, let. c, LPD, il s'agit notamment du droit à l'effacement ou à la destruction des données personnelles traitées de manière illicite (voir question 7.1).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6687 ss.

9. Dispositions particulières pour le traitement de données personnelles par des organes fédéraux

Remarque : Contrairement aux responsables du traitement privés (voir question 8), les organes fédéraux ne sont généralement en droit de traiter des données personnelles que si une base légale le prévoit. L'OFJ a publié deux outils pour l'élaboration de ces bases légales :

- Guide de législation en matière de protection des données
- Note sur la révision totale de la LPD — Aperçu des principales modifications en vue de l'élaboration des bases légales concernant le traitement de données par les organes fédéraux

10. Préposé fédéral à la protection des données personnelles et à la transparence (PFPDT)

Question : *En quoi la révision totale de la LPD renforce-t-elle l'indépendance et les compétences en matière de surveillance du PFPDT ?*

Plusieurs mesures ont été prises pour renforcer l'indépendance du PFPDT : désormais, ce dernier dispose de son propre budget (art. 43, al. 5, 1re phrase, et 45 LPD) et son chef est élu par l'Assemblée fédérale (Chambres réunies) (art. 43, al. 1, LPD).

Ses compétences en matière de surveillance ont par ailleurs été étendues. Selon la nouvelle LPD, le PFPDT ouvre d'office ou sur dénonciation une enquête si des indices suffisants font penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données (art. 49, al. 1, LPD). Il peut renoncer à ouvrir une enquête lorsque la violation est de peu d'importance (art. 49, al. 2, LPD). Les pouvoirs d'enquête du PFPDT sont également renforcés (art. 50 LPD). Si le PFPDT conclut que des dispositions de protection des données sont violées, il peut désormais non seulement émettre une recommandation, mais aussi rendre une décision susceptible de recours (art. 51 LPD). Il peut par exemple ordonner la modification, la suspension ou la cessation d'un traitement ainsi que l'effacement ou la destruction de données personnelles. Si la personne concernée est l'auteur de la dénonciation, le PFPDT l'informe des suites données à celle-ci et du résultat d'une éventuelle enquête (art. 49, al. 4, LPD).

Vous trouverez de plus amples informations sur le statut et les tâches du PFPDT sur son site web : https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/grundlagen/rolle-edoeb.html

11. Dispositions pénales

11.1 Vue d'ensemble

Question : *Quelles modifications ont été apportées aux dispositions pénales dans le cadre de la révision totale de la LPD ?*

Outre un renforcement de la surveillance de la protection des données, le durcissement des dispositions pénales doit permettre d'assurer un meilleur respect de la législation sur la protection des données. C'est la raison pour laquelle la nouvelle LPD couvre davantage d'infractions et la limite maximale des amendes en cas de violation des prescriptions est passée de 10 000 à 250 000 francs (art. 60 ss LPD).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6713 ss.

11.2 Destinataires des dispositions pénales

Question : *Pourquoi les dispositions pénales de la LPD ne visent-elles pas les entreprises, mais les personnes physiques au sein des entreprises ?*

Il est vrai que les dispositions pénales de la LPD visent en premier lieu les personnes physiques, mais il ne s'agit pas là d'une particularité de cette loi. En droit suisse, les destinataires des dispositions pénales sont essentiellement des personnes physiques et pas des entreprises.

Toutefois, l'art. 6 de la loi fédérale sur le droit administratif (DPA ; RS 313.0), en particulier, en relation avec l'art. 64, al. 1, LPD, garantit que, en cas de violation d'obligations qui ne concernent que les entreprises, ce ne soit pas la responsabilité pénale des simples collaborateurs qui soit engagée, mais celle des dirigeants. Cela signifie que ce sont avant tout les chefs d'entreprise, les organes ou les membres des organes, les associés gérants ainsi que les dirigeants effectifs qui sont responsables. Dans tous les cas, la personne doit disposer d'un pouvoir de décision autonome dans un domaine déterminé de l'entreprise.

Exemple : L'obligation de se renseigner sur le niveau de protection des données assuré par un sous-traitant (art. 61, let. b, LPD) incombe aux dirigeants de l'entreprise et non aux « simples collaborateurs ». En revanche, si un collaborateur se rend coupable d'une violation de son devoir de discrétion (art. 62 LPD), il devra lui-même rendre des comptes.

Lorsque l'amende entrant en ligne de compte ne dépasse pas 50 000 francs et que l'enquête rendrait nécessaires à l'égard des personnes punissables des mesures d'instruction hors de proportion avec la peine encourue, l'autorité compétente peut renoncer à poursuivre ces personnes et condamner l'entreprise au paiement de l'amende à leur place (art. 64, al. 2, LPD).

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6713 ss.

11.3 Compétence en matière de poursuite pénale

Question : *À qui incombe la compétence en matière de poursuite pénale ?*

La poursuite et le jugement d'actes punissables en vertu de la LPD n'incombent pas au PFPDT. Contrairement à (la plupart de) ses homologues européens, le PFPDT n'a donc pas le pouvoir d'infliger des sanctions. Ce sont les autorités cantonales de poursuite pénale (police, ministère public, tribunaux pénaux ; art. 65, al. 1, LPD) qui sont compétentes en la matière, comme c'était déjà le cas sous l'ancien droit. Le PFPDT peut néanmoins dénoncer des infractions aux

autorités de poursuite pénale compétentes et faire valoir les droits d'une partie plaignante dans la procédure (art. 65, al. 2, LPD). Il peut par ailleurs mentionner sur ses décisions la sanction prévue par l'art. 63 LPD : en vertu de cette disposition, les personnes privées qui, intentionnellement, ne se conforment pas à une décision du PFPDT sont punies d'une amende de 250 000 francs au plus. Dans ce cas de figure, la poursuite pénale incombe toutefois aussi aux autorités cantonales de poursuite pénale.

Référence : Message concernant la révision totale de la LPD, FF 2017 6565, p. 6718 ss.

12. Développements internationaux en matière de protection des données

12.1 Directive (UE) 2016/680

Question : *Quelle importance revêt la directive (UE) 2016/680 pour la Suisse ?*

La directive (UE) 2016/680 constitue un développement de l'acquis de Schengen que la Suisse a dû reprendre en vertu de l'accord d'association à Schengen. Elle a un champ d'application spécifique et régit le traitement de données par les autorités à des fins de poursuite pénale, d'exécution de sanctions pénales et de prévention des risques sécuritaires.

12.2 Règlement général de l'UE sur la protection des données et décision d'adéquation

12.2.1 **Question** : *Quelle importance revêt le règlement général de l'UE sur la protection des données pour la Suisse ?*

Le règlement général de l'UE sur la protection des données (RGPD) se compose de dispositions générales relatives à la protection des données traitées par des particuliers ou des autorités dans les États membres de l'UE. Contrairement à la directive (UE) 2016/680 (voir question 12.1), il ne constitue pas un développement de l'acquis de Schengen et n'est pas directement contraignant pour la Suisse. Cela dit, il s'applique aux entreprises sises en Suisse si elles proposent des marchandises ou des services à des personnes qui se trouvent dans l'un des pays de l'UE ou si elles analysent leur comportement (profilage). Il est par ailleurs important pour la Suisse de continuer d'être reconnue par l'UE comme un État tiers ayant un niveau de protection adéquat des données sous le régime du RGPD.

12.2.2 **Question** : *Le droit suisse de la protection des données satisfait-il aux normes européennes ?*

La Suisse dispose depuis l'année 2000 d'une décision d'adéquation de l'UE lui reconnaissant un niveau de protection des données équivalent. L'adéquation aux prescriptions européennes en matière de protection des données fait l'objet de vérifications périodiques. Le nouveau droit permet de rapprocher le niveau de protection suisse des standards de l'UE et a conduit l'UE à confirmer que la Suisse offre un niveau adéquat de protection des données (voir le rapport du 15 janvier 2024 de la Commission européenne ainsi que le document de travail contenant les rapports par pays qui l'accompagne, ce dernier document n'est cependant disponible qu'en anglais).

12.2.3 **Question** : *Quelles seraient les conséquences si la Commission européenne venait à conclure que le niveau de protection des données en Suisse n'était plus suffisant ?*

En l'absence du maintien de la décision d'adéquation de l'UE, les transmissions de données vers la Suisse ne seraient possibles que si des garanties appropriées et certains cas d'excep-

tion étaient prévus. Il en découlerait des obstacles administratifs considérables, qui mettraient un frein au libre flux des données et, partant, à l'innovation, pénalisant ainsi la place économique suisse. L'UE a confirmé le 15 janvier 2024 que la Suisse offre un niveau adéquat de protection des données (voir le rapport du 15 janvier 2024 de la Commission européenne ainsi que le document de travail contenant les rapports par pays qui l'accompagne, ce dernier document n'est cependant disponible qu'en anglais).

12.3 Convention 108+ pour la protection des personnes à l'égard du traitement des données à caractère personnel du Conseil de l'Europe

Question : *Pourquoi la Suisse a-t-elle adhéré à la Convention modernisée 108+ du Conseil de l'Europe ?*

Une cinquantaine d'États, dont la Suisse, ont jusqu'ici ratifié la Convention 108 du Conseil de l'Europe. Conclue en 1981, elle est le premier instrument contraignant de droit international en matière de protection des données. Le Conseil de l'Europe a décidé de l'adapter à l'ère numérique. La Suisse a ratifié la version révisée ou Convention modernisée 108 (Convention 108+) le 7 septembre 2023 ; la Convention 108+ n'entrera toutefois en vigueur que lorsque 38 Etats parties l'auront ratifiée. La Suisse peut ainsi continuer d'afficher un haut niveau de protection des données vis-à-vis de ses partenaires internationaux, ce qui renforce son économie. La révision totale de la LPD visait notamment une mise en conformité avec les exigences de la Convention 108+.