Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

La Communication de données à l'étranger en 24 questions

A l'intention des autorités fédérales et du secteur privé

(dernières modifications: September 2014)

1) Pourquoi a-t-on révisé les dispositions de la loi fédérale sur la protection des données (LPD) relatives à la communication de données à l'étranger?

On a procédé à cette révision pour adapter le droit suisse de la protection des données au Protocole additionnel à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (Convention STE 108).

Les objectifs sont les suivants:

- garantir entre tous les États parties non seulement un niveau de protection des données comparable et aussi élevé que possible, mais aussi la libre circulation des données;
- faire en sorte que la communication de données à caractère personnel à un destinataire qui n'est pas concerné par la Convention ne puisse se faire que si l'État ou l'organisation destinataire garantit un niveau de protection adéquat.

2) Où et comment la communication de données à l'étranger est-elle réglementée dans la LPD?

La disposition-clé régissant la communication de données à l'étranger est l'art. 6 LPD. D'autres dispositions de la LPD et de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD) complètent cet article ou en constituent des dispositions d'exécution. Le libellé de l'art. 6 LPD est le suivant:

[1] Aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une législation assurant un niveau de protection adéquat.

[2] En dépit de l'absence d'une législation assurant un niveau de protection adéquat à l'étranger, des données personnelles peuvent être communiquées à l'étranger, à l'une des conditions suivantes uniquement:

a. des garanties suffisantes, notamment contractuelles, permettent d'assurer un niveau de protection adéquat à l'étranger;
b. la personne concernée a, en l'espèce, donné son consentement;
c. le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et les données traitées concernent le cocontractant;
d. la communication est, en l'espèce, indispensable soit à la sauvegarde d'un intérêt public prépondérant, soit à la constatation, l'exercice ou la défense d'un droit en justice;
e. la communication est, en l'espèce, nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée;
f. la personne concernée a rendu les données accessibles à tout un chacun et elle ne s'est pas opposée formellement au traitement;
g. la communication a lieu au sein d'une même personne morale ou société ou entre des personnes morales ou sociétés réunies sous une direction unique, dans la mesure où les parties sont soumises à des règles de protection des données qui garantissent un niveau de protection adéquat.

[3] Le Préposé fédéral à la protection des données et à la transparence (préposé, art. 26) doit être informé des garanties données visées à l'al. 2, let. a, et des règles de protection des données visées à l'al. 2, let. g. Le Conseil fédéral règle les modalités du devoir d'information.

Feldeggweg 1, 3003 Bern
Tel. 058 462 43 95, Fax 058 465 99 96
www.edoeb.admin.ch

3) En quoi la nouvelle réglementation a-t-elle changé sur le plan terminologique?

Sur le plan terminologique, la LPD a été adaptée au Protocole additionnel en ce sens que l'exigence de l'équivalence du niveau de protection a été remplacée par celle de l'adéquation du niveau de protection. Sur le fond, cela ne signifie cependant pas que la nouvelle réglementation est plus sévère ou moins sévère que l'ancienne en ce qui concerne les exigences relatives à la communication transfrontière de données.

4) La publication de données personnelles sur Internet est-elle assimilée à une communication de données à l'étranger?

La publication de données personnelles au moyen de services d'information et de communication automatisés comme Internet afin d'informer le public n'est pas assimilée à une communication de données à l'étranger (art. 5 OLPD). Les autres exigences relevant de la protection des données sont réservées. Les organes fédéraux ne sont notamment en droit de communiquer des données que s'il existe une base légale (art. 19 LPD).

5) Pour quelles raisons communique-t-on des données personnelles à l'étranger?

Voici trois raisons parmi d'autres:

- le besoin de centraliser une activité de traitement de données;
- l'externalisation de traitements de données;
- la reprise d'une société par une entreprise étrangère.

6) Que signifie le devoir de diligence du maître d'un fichier en cas de communication de données à l'étranger, et quels sont les différents types de devoir de diligence?

Le devoir de diligence signifie:

- respecter les principes généraux de protection des données qui figurent dans la LPD (devoir général de diligence);
- garantir l'adéquation de la protection des données dans le pays destinataire pour chaque communication (devoir spécial de diligence);
- informer le PFPDT en vertu de l'art. 6, al. 3, LPD (devoir spécial de diligence).

7) Quels sont les principes de protection des données qui doivent être respectés en vertu du devoir général de diligence?

Les personnes privées qui communiquent des données personnelles à l'étranger doivent:

1. justifier cette communication (art. 13, al. 1, LPD). Au nombre des motifs justificatifs, on compte:
    a. le consentement de la ou des personnes concernées,
    b. un intérêt prépondérant public ou privé, par exemple la centralisation des données relatives à des clients ou de la gestion des salaires d'employés, ou
    c. une base légale;
2. contrôler la licéité de la communication des données (art. 4, al. 1, LPD). Une communication est illicite si elle est contraire notamment à des dispositions du droit suisse;
3. rendre la future communication des données reconnaissable pour les personnes concernées (principe de la bonne foi, art. 4, al. 2 et 4, LPD);
4. garantir la proportionnalité et l'opportunité de la communication des données (art. 4, al. 2 et 3, LPD).

Exemple: l'entreprise qui veut centraliser la gestion des salaires à l'étranger ne doit communiquer que les données relatives aux salaires, lesquelles ne devront être traitées que dans le but qui a été indiqué;

5. garantir l'exactitude des données (art. 5 LPD);
6. prendre les mesures techniques et organisationnelles propres à garantir l'intégrité, la confidentialité et la disponibilité des données lors de la communication (art. 7 LPD).

8) Quels sont les principes de protection des données qui doivent être respectés en vertu du devoir spécial de diligence?

Il incombe au maître d'un fichier:

- de déterminer si le niveau de protection est adéquat dans le pays destinataire (art. 6, al. 1, LPD);
- de respecter les conditions alternatives si le niveau de protection dans le pays destinataire n'est pas adéquat (art. 6, al. 2, LPD);
- d'informer le PFPDT en vertu de l'art. 6, al. 3, LPD.

9) De quoi faut-il tenir compte au moment où l'on détermine si le niveau de protection est adéquat dans le pays destinataire (art. 6, al. 1, LPD)?

Le maître d'un fichier doit examiner si les prescriptions juridiques de nature générale ou sectorielle en vigueur dans l'État destinataire et si la pratique juridique de ce dernier tiennent compte des principes inscrits dans la Convention STE 108 et dans le Protocole additionnel.

Il doit notamment déterminer:

- si les principes figurant dans la LPD sont respectés;
- si la personne concernée peut défendre ses intérêts en cas de non-respect de ces principes;
- si le droit d'accès est garanti, et
- s'il existe un organe de surveillance indépendant.

Depuis la signature de l'accord américano-suisse sur les principes de la sphère de sécurité (U.S.-Swiss Safe Harbor Framework, http://www.export.gov/safeharbor/), les États-Unis font aussi partie des États qui garantissent, à certaines conditions, un niveau de protection des données adéquat au sen de l'art. 6, al. 1, LPD. Les entreprises américaines peuvent s'engager à respecter les principes de la protection des données qui sont consacrés dans l'accord en s'enregistrant auprès du Ministère américain du commerce. Avant que des données personnelles soient transmises à une entreprise américaine, le préposé recommande de consulter la liste des entreprises enregistrées (https://safeharbor.export.gov/swisslist.aspx) tenue par le Bureau américain du commerce international (International Trade Administration, ITA) et de convenir le cas échéant de dispositions complémentaires sur la protection des données.

10) Quel rôle la «liste des États dotés d'une loi sur la protection des données assurant un niveau de protection adéquat» – liste publiée par le PFPDT – joue-t-elle dans cette question?

Le maître du fichier peut se servir de la liste d'États publiée par le PFPDT pour examiner si le niveau de protection est adéquat (art. 31, al. 1, let. d, LPD et art. 7 OLPD). La liste énumère les États:

- qui sont parties à la Convention STE 108 et à son Protocole additionnel, ou
- qui, de l'avis du PFPDT, disposent d'une législation sur la protection des données assurant un niveau de protection adéquat.

La liste est actualisée en permanence mais n'est pas exhaustive. Si un État n'y figure pas, cela ne signifie pas forcément qu'il ne dispose pas d'une législation sur la protection des données assurant un niveau de protection adéquat.

Par ailleurs, les personnes privées ou les organes fédéraux qui communiquent des données à quelqu'un se trouvant dans un État figurant sur la liste peuvent partir de l'idée qu'ils agissent en toute bonne foi. Par contre, s'ils savent par exemple, sur la base d'expériences pratiques, que les prescriptions relatives à la protection des données ne sont pas observées dans un tel État, que ce soit de façon générale ou dans certains domaines, ils ne sont plus de bonne foi. En pareil cas, la communication ne doit intervenir qu'aux conditions spécifiées à l'art. 6, al. 2, LPD.

11) Que vise l'art. 6, al. 2, LPD?

Si le niveau de protection offert par la législation du pays destinataire n'est pas adéquat, les données ne doivent être communiquées que si les conditions fixées à l'art. 6, al. 2, LPD sont remplies.

Exemple: Si la législation du pays destinataire n'offre un niveau de protection adéquat que pour les données concernant les personnes physiques, des garanties au sens de l'art. 6, al. 2, let. a et g, LPD doivent être fournies pour la communication de données concernant des personnes morales. Si ces garanties font défaut, la communication des données à l'étranger pourra toutefois se faire pour autant que l'un des motifs justificatifs énumérés à l'art. 6, al. 2, let. b à f, LPD soit rempli.

12) Quels sont les contrats qui peuvent servir de motif justificatif pour la communication de données (art. 6, al. 2, let. a, LPD)?

Les contrats-modèles ou les clauses standard que le PFPDT a établis ou reconnus (art. 6, al. 3, OLPD) sont les suivants:

- les **clauses contractuelles types de l'Union européenne**: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm
- le **contrat-type du Conseil de l'Europe** visant à assurer une protection équivalente des données dans le cadre des flux transfrontières des données: http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/ContratType_1992.pdf
- le **contrat-type du PFPDT** pour l'externalisation (outsourcing) du traitement de données à l'étranger: http://www.edoeb.admin.ch/datenschutz/00626/00743/00858/00859/index.html?lang=fr ;

  NB: en cas d'externalisation, le but du traitement reste le même tant pour le mandant que pour le mandataire. Le mandant reste par ailleurs le seul et unique maître du fichier, car il est le seul à décider du but et du contenu dudit fichier (cf. art. 3, let. i, LPD).

  Exemple: la gestion des salaires est confiée à un mandataire à l'étranger.

  Par contre, s'il ne s'agit pas d'une externalisation, le destinataire d'une communication de données remplace souvent le but initial d'un traitement de données par un nouveau but. Il devient ainsi également le maître du fichier au sens de la LPD.

  Exemple: les données relatives à des clients dont le traitement servait initialement exclusivement à gérer les relations avec lesdits clients sont désormais aussi communiquées et traitées à des fins de marketing.

Les personnes ou les organes fédéraux qui veulent communiquer des données peuvent aussi utiliser d'autres formes de contrat ou de garantie, par exemple un contrat spécifique de protection des données ou des clauses de protection des données figurant dans d'autres contrats. Ces clauses doivent garantir un niveau de protection adéquat, c'est-à-dire conforme à la LPD.
Elles doivent englober la totalité des indications nécessaires à la communication des données, en particulier:

- l'identité de l'expéditeur et du destinataire des données;

- les catégories correspondant aux données à communiquer;
- les buts de la communication;
- les catégories dans lesquelles sont classées les personnes concernées;
- les destinataires finaux des données et la durée de conservation de ces dernières.

Les clauses de protection des données doivent en outre:

- permettre le respect des principes régissant la protection des données;
- garantir les droits des personnes concernées, à savoir le droit d'accès, le droit de rectification et le droit d'agir en justice; prévoir un mécanisme de contrôle;
- prévoir des mesures destinées à garantir la sécurité et la confidentialité lors de la communication de données sensibles ou de profils de la personnalité.

13) Quelles sont les conditions et les caractéristiques du consentement à la communication de données à l'étranger (art. 6, al. 2, let. b, LPD)?

Le consentement doit:

- porter sur un cas particulier, c'est-à-dire sur une situation concrète. Consentir de façon générale à la communication régulière et systématique de données à l'étranger à des fins diverses et dans différentes situations est tout simplement illicite. À titre exceptionnel, l'expression «en l'espèce» peut englober non seulement une seule communication transfrontière de données, mais aussi un ensemble de communications, si les conditions (en particulier le but et le destinataire) restent les mêmes.

  Exemple: communiquer plusieurs procès-verbaux d'un groupe de travail dont font partie des personnes provenant de différents pays, sans qu'il faille requérir leur consentement pour la communication de chaque document.
- être donné librement;
- être donné après que la personne concernée a été dûment informée (art. 4, al. 5, LPD);
- être explicite si la communication porte sur des données sensibles;
- pouvoir être retiré à tout moment pour de futurs traitements ou communications de données.

Le consentement ne libère par le maître du fichier de son devoir de diligence, notamment en ce qui concerne les mesures portant sur la sécurité des données ou le fait de s'assurer que le destinataire des données respecte le but fixé.

14) Qu'entend-on par communication de données en relation directe avec la conclusion ou l'exécution d'un contrat (art. 6, al. 2, let. c, LPD)?

Un partenaire contractuel communique des données personnelles concernant son cocontractant à un tiers à l'étranger en vue de la conclusion ou exécution d'un contrat.

Exemples:

- une agence de voyages communique des données concernant des clients à un hôtel à l'étranger;
- quelqu'un communique des données à des sociétés de renseignements commerciaux en vue d'un examen de la solvabilité dans le cadre de contrats de vente;
- des commissionnaires-expéditeurs communiquent des données à des entreprises de transport dans le cadre de contrats de livraison;

- des agences de voyage communiquent des données à des entreprises de transport dans le cadre de prestations de transport internationales (voyages en train, en bateau ou en avion);
- quelqu'un communique des données dans le cadre de transactions bancaires ou de mandats relevant du trafic des paiements à l'échelle internationale.

15) Quand et à quelles conditions la communication de données visée à l'art. 6, al. 2, let. d, LPD entre-t-elle en ligne de compte?

Dans ce cas de figure, la communication de données doit:

- être justifiée par un intérêt public prépondérant ou par des exigences inhérentes à une procédure judiciaire;
- être indispensable à la sauvegarde de cet intérêt;
- intervenir dans un cas concret, c'est-à-dire dans une situation précise.

Exemple: Pour des raisons de sécurité, une association de football communique des données personnelles relatives à des hooligans à l'entité responsable dans le pays où elle va aller disputer un match.

Par ailleurs, on n'est pas forcément en présence d'un intérêt prépondérant lorsqu'un État motive sa demande de communication de données par la lutte contre le terrorisme, mais qu'il pourrait utiliser ces données à des fins illicites (par exemple pour commettre des violations des droits de l'homme).

16) À quelles conditions la communication de données visée à l'art. 6, al. 2, let. e, LPD est-elle licite?

En vertu de cette disposition, les données peuvent être communiquées:

- si des intérêts vitaux de la personne concernée sont en jeu;
- si la personne concernée n'est pas en mesure de faire valoir ses propres intérêts (par exemple à la suite d'un accident survenu à l'étranger);
- si l'on présume que la personne concernée va donner son consentement à la communication des données.

Les données concernant des proches de la personne concernée peuvent aussi être communiquées si ces personnes ne peuvent pas donner leur consentement et si, à défaut, la vie de la personne concernée serait en danger.

17) Comment peut-on limiter la communication de données rendues accessibles à tout un chacun (art. 6, al. 2, let. f, LPD)?

La personne qui a rendu les données la concernant accessibles à tout un chacun mais qui ne souhaite pas que ces données soient traitées sans restriction doit indiquer expressément les buts pour lesquels les données peuvent être traitées. Il est par ailleurs envisageable que la personne concernée indique à une personne précise qui traite des données qu'elle ne souhaite pas que soient traitées les données publiées qui la concernent (cf. art. 12, al. 2, let. b, LPD).

18) Quelles conditions les règles de protection des données en vigueur dans les groupes de sociétés doivent-elles remplir (art. 6, al. 2, let. g, LPD)?

Les règles de protection des données en vigueur dans les groupes de sociétés doivent remplir les conditions suivantes pour pouvoir compenser l'absence d'un niveau de protection des données adéquat:

- sur le fond, elles doivent remplir au moins les conditions applicables aux personnes privées traitant des données, conditions qui figurent dans la Convention STE 108 et dans son Protocole additionnel (cf. à ce propos le commentaire de l'art. 6, al. 2, let. a, LPD);
- le caractère contraignant des règles en vigueur dans les groupes de sociétés doit être garanti sur le plan formel et lors de l'application pratique. Le côté formel du caractère contraignant peut être conféré par exemple par une décision du conseil d'administration. L'application pratique peut être garantie par exemple par des audits.

Autres règles régissant la communication de données au sens de l'art. 6, al. 2, let. g, LPD:

- le maître du fichier n'est pas libéré de l'obligation de respecter les autres dispositions de la LPD pour les traitements de données qui sont effectués en Suisse;
- les différentes sociétés qui constituent le groupe doivent reprendre les règles et les appliquer.

19) Quand le PFPDT doit-il être informé d'une communication de données?

Il y a lieu d'informer le PFPDT (art. 6, al. 3, LPD et art. 6, al. 1, OLPD):

- en cas de communication de données au sens de l'art. 6, al. 2, let. a, LPD (garantie de la protection des données par un contrat);
- en cas de communication de données au sens de l'art. 6, al. 2, let. g, LPD (garantie de la protection des données par des règles internes aux groupes de sociétés).

20) Comment le PFPDT doit-il être informé?

- L'information consiste en l'envoi d'une copie des garanties ou des règles de protection des données convenues avec le destinataire.
- En cas d'utilisation de contrats-types ou de clauses contractuelles standard, le maître du fichier doit simplement informer le PFPDT de cette utilisation, sans entrer dans les détails. Si le maître du fichier utilise d'autres garanties dans certains cas ou pour certaines parties de la communication des données, il doit en informer le PFPDT au moyen d'une copie.
- Après la première information, le devoir d'information est considéré comme rempli pour toutes les communications suivantes qui se basent sur les mêmes garanties ou règles de protection des données, pour autant que les catégories de destinataires, les finalités du traitement et les catégories de données à communiquer soient essentiellement les mêmes.
- Le PFPDT ne doit pas être informé de chaque courriel ou de chaque courrier postal envoyé à l'étranger. Le devoir d'information ne s'applique pas aux envois à caractère privé ou personnel.
- Le maître du fichier informe le PFPDT avant la communication des données à l'étranger. S'il ne peut pas le faire, il s'acquitte de son obligation dès que possible.
- L'information peut se faire par Internet.
- Les formulaires de déclaration utilisés en vertu de l'ancienne LPD ont été supprimés.
- La violation du devoir d'information entraîne des sanctions pénales (art. 34, al. 2, let. a, LPD).

21) En quoi consiste l'examen effectué par le PFPDT?

- En cas d'utilisation de contrats-types reconnus pour la communication de données à l'étranger, le PFPDT n'effectue aucun examen du dispositif réglementaire; il se limite à en prendre connaissance.
- Si aucun contrat-type n'est utilisé ou si des éléments essentiels de ces contrats-types ont été modifiés, le PFPDT peut examiner le dispositif réglementaire. Le PFPDT a 30 jours pour effectuer son examen (art. 6, al. 5, OLPD).
- Si les garanties et les règles n'assurent pas un niveau de protection des données adéquat, le PFPDT peut prendre contact avec le maître du fichier et, si nécessaire, édicter une recommandation au sens de l'art. 29 LPD.
- Si le PFPDT ne réagit pas dans le délai légal, le maître du fichier peut considérer que le PFPDT n'a aucune objection à formuler contre les garanties et les règles de protection des données qui lui ont été présentées.

22) Quelles sont les conséquences d'une violation du devoir de diligence?

Le maître d'un fichier répond des préjudices causés par une violation de son devoir de diligence. Il doit notamment prouver qu'il a pris toutes les mesures nécessaires pour assurer un niveau de protection des données adéquat. L'ordonnance concrétise cet aspect du devoir de diligence en obligeant le maître du fichier à prendre les mesures adéquates pour garantir que le destinataire respecte les garanties et les règles de protection des données concernées (art. 6, al. 4, OLPD).

23) La personne concernée peut-elle dénoncer la violation du devoir de diligence?

La personne concernée peut, en vertu de l'art. 15, al. 1, LPD, porter devant la justice tout cas de communication illicite de données à l'étranger.

24) Un fichier contenant des données personnelles qui sont communiquées régulièrement à des tiers à l'étranger doit-il être déclaré en vertu de l'art. 11a LPD?

Oui, un tel fichier doit être déclaré au PFPDT en vertu de l'art. 11a, al. 3, let. b, LPD. La déclaration vise à établir la transparence des fichiers contenant des données qui sont régulièrement communiquées à des tiers.

L'information du PFPDT prévue à l'art. 6, al. 3, LPD à propos de la communication de données à l'étranger est réservée.