Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Explications relatives à la communication de données personnelles à l'étranger suite à la révision de la loi fédérale sur la protection des données

(dernières modifications: Janvier 2017)

1. Contexte historique

1.1 Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention STE 108)

La Suisse a ratifié la Convention STE 108 (RS 0.235.1) en 1997 avant de la mettre en vigueur avec effet au 1er février 1998. Depuis cette date, la loi fédérale sur la protection des données (LPD) et les lois cantonales sur la protection des données doivent satisfaire aux nouvelles exigences. Les principes inscrits dans la Convention STE 108 visent à 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. Aucune partie à la Convention STE 108 n'est autorisée à interdire le transfert d'informations vers une partie qui offre la protection minimale prévue par la Convention.

Les principes figurant dans la Convention STE 108 ont été repris à l'échelle de l'Union européenne dans la directive 95/46/CE (http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_fr.pdf).

La disposition de la Convention STE 108 qui concerne les flux transfrontières de données a la teneur suivante:

Art. 12 Flux transfrontières de données à caractère personnel et droit interne

1. Les dispositions suivantes s'appliquent aux transferts à travers les frontières nationales, quel que soit le support utilisé, de données à caractère personnel faisant l'objet d'un traitement automatisé ou rassemblées dans le but de les soumettre à un tel traitement.

2. Une Partie ne peut pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel à destination du territoire d'une autre Partie.

3. Toutefois, toute Partie a la faculté de déroger aux dispositions du par. 2:

a. dans la mesure où sa législation prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel, en raison de la nature de ces données ou de ces fichiers, sauf si la réglementation de l'autre Partie apporte une protection équivalente;

b. lorsque le transfert est effectué à partir de son territoire vers le territoire d'un Etat non contractant par l'intermédiaire du territoire d'une autre Partie, afin d'éviter que de tels transferts n'aboutissent à contourner la législation de la Partie visée au début du présent paragraphe.

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

1.2 Protocole additionnel à la Convention 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

En 2001, le Conseil de l'Europe a adopté un Protocole additionnel (FF 2003 1977) concernant les autorités de contrôle et les flux transfrontières de données, lequel vise à améliorer la mise en œuvre de la Convention STE 108. Cette amélioration s'est révélée nécessaire notamment en raison du volume croissant des flux transfrontières de données. Le Protocole additionnel renforce les exigences dans deux domaines qui étaient insuffisamment réglementés, comme l'a montré la pratique. D'une part, il s'agit d'éviter que des transferts de données à destination d'États ou d'entités tiers n'amènent à contourner la législation de l'État d'origine partie à la Convention STE 108. D'autre part, le Protocole additionnel prévoit que le transfert de données à caractère personnel vers un destinataire qui n'est pas régi par la Convention STE 108 ne peut être effectué que si l'État ou l'organisation destinataire assure un niveau de protection adéquat. Les garanties peuvent notamment résulter de clauses contractuelles, pour autant qu'elles soient jugées suffisantes. La Suisse a ratifié le Protocole additionnel à la fin de l'année 2007. L'art. 2 du Protocole additionnel a la teneur suivante:

Art. 2 Flux transfrontières de données à caractère personnel vers un destinataire n'étant pas soumis à la juridiction d'une Partie à la Convention

1. Chaque Partie prévoit que le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un Etat ou d'une organisation qui n'est pas Partie à la Convention ne peut être effectué que si cet Etat ou cette organisation assure un niveau de protection adéquat pour le transfert considéré.

2. Par dérogation au par. 1 de l'art. 2 du présent Protocole, chaque Partie peut autoriser un transfert de données à caractère personnel:

a. si le droit interne le prévoit:

- *pour des intérêts spécifiques de la personne concernée, ou*
- *lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants, ou*

b. si des garanties pouvant notamment résulter de clauses contractuelles sont fournies par la personne responsable du transfert, et sont jugées suffisantes par les autorités compétentes, conformément au droit interne.

2. mise en œuvre du protocole additionnel dans le droit suisse

La version révisée de la LPD, qui est entrée en vigueur le 1er janvier 2008, a été adaptée au Protocole additionnel du Conseil de l'Europe pour ce qui est de la communication transfrontière de données. La disposition-clé régissant la communication de données à l'étranger est l'art. 6 LPD. D'autres dispositions des versions révisées de la LPD et de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD, RS 235.11) complètent cet article ou en constituent des dispositions d'exécution; avec l'art. 6 LPD, elles forment la nouvelle réglementation régissant la communication de données à l'étranger. Elles font également l'objet d'un commentaire dans le présent document.
L'art. 6 LPD a la teneur suivante:

Art. 6 Communication transfrontière de données

[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.

2.1 Remarques générales concernant la communication de données à l'étranger suite à la révision de la LPD

2.1.1 Définitions et raisons d'une communication de données à l'étranger

On parle de communication de données à l'étranger quand des données personnelles quittent le territoire suisse parce qu'elles sont communiquées par le maître du fichier dans lequel elles se trouvent ou parce qu'elles sont consultées par leur destinataire à l'étranger au moyen d'une procédure d'appel.

La publication de données personnelles au moyen de services d'information et de communication automatisés afin d'informer le public, par exemple sur Internet, n'est pas assimilée à une communication de données à l'étranger (art. 5 OLPD) bien que ces informations puissent aussi être consultées à l'étranger. Il va de soi que, dans ce cas de figure, il convient de respecter les autres exigences qui découlent notamment du droit de la protection des données et de la personnalité. L'art. 19 OLPD dispose que l'art. 6 OLPD s'applique aussi aux organes fédéraux. Ces derniers sont du reste tenus de respecter les conditions inscrites dans la législation sur la protection des données et applicables au traitement de données par les organes fédéraux, notamment celle qui prévoit que les communications de données doivent reposer sur des bases légales (art. 19 LPD).

Les raisons pour lesquelles des données personnelles sont communiquées à l'étranger sont notamment la centralisation ou l'externalisation d'un traitement de données déterminé, mai aussi la reprise d'une entreprise par une société étrangère.

2.1.2 Le devoir de diligence et le devoir d'information remplacent l'obligation de déclarer

L'obligation de déclarer les communications de données à l'étranger a été remplacée par un devoir de diligence. D'une manière générale, cela signifie que les personnes privées et les organes fédéraux qui communiquent des données à l'étranger sont tenus de respecter les principes généraux figurant dans la LPD et de s'assurer que la protection est adéquate dans le pays destinataire. Si la protection n'est pas adéquate, une des garanties énumérées à l'art. 6, al. 2, LPD doit être fournie. Pour déterminer si une communication de données est conforme à la protection des données, il convient de tenir compte des tenants et des aboutissants de la communication. La protection doit faire l'objet d'une évaluation au cas par cas, pour chaque communication ou catégorie de communication.

Le devoir de diligence est par ailleurs assorti d'un devoir d'information qui ne doit cependant être rempli que ponctuellement et qui a été simplifié en pratique, contrairement à l'obligation de déclarer qui existait auparavant (art. 6, al. 3, LPD). Il y a lieu d'opérer une distinction entre le devoir général de

diligence et le devoir simplifié de diligence. Le devoir général de diligence englobe le respect des principes suivants (à propos du devoir spécial de diligence, voir les explications figurant au ch 3.1.2):

La communication de données à l'étranger doit être licite (art. 4, al. 1, LPD) et reposer sur un motif justificatif (art. 13 LPD), qu'il s'agisse du consentement de la personne concernée, d'un intérêt prépondérant public ou privé ou d'une base légale. On pourrait citer comme exemples d'intérêt prépondérant privé la centralisation de la gestion des salaires, des données concernant des candidats ou des curriculum vitae de collaborateurs en vue de planifier leur développement.

Une communication est illicite si elle est contraire notamment à des dispositions du droit suisse. La communication doit en outre être faite dans le respect du principe de la bonne foi, elle doit être proportionnelle et elle doit avoir un but bien défini (art. 4, al. 2 et 3, LPD). En d'autres termes, la communication de données et ses buts doivent être reconnaissables pour la personne concernée. Les données qui doivent être communiquées doivent être nécessaires et appropriées pour atteindre les buts indiqués. En outre, la violation de la personnalité résultant de la communication doit avoir un rapport raisonnable avec le but visé (proportionnalité et opportunité). Si l'on veut par exemple centraliser la gestion des salaires à l'étranger, il ne faut communiquer que les données ayant trait aux salaires.

La proportionnalité joue aussi un rôle en rapport avec la durée de conservation des données. Les données à communiquer doivent en outre être exactes (art. 5 LPD). Enfin, il convient de prendre des mesures techniques et organisationnelles pour protéger les données lors de la communication (art. 7 LPD), c'est-à-dire des mesures propres à garantir l'intégrité, l'authenticité et la disponibilité des données lors de la communication.

3. Les modifications en détail

3.1 Les modifications de l'art. 6, al. 1, LPD

3.1.1 L'adéquation remplace l'équivalence du niveau de protection à l'étranger

Le principe selon lequel des données ne doivent pas être communiquées à l'étranger si cela risque de menacer gravement la personnalité des personnes concernées, notamment parce que le niveau de protection ne correspond pas à celui qui existe en Suisse, est maintenu. Sur le plan terminologique, l'art. 6, al. 1, LPD a été adapté à l'art. 2, par. 1, du 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.

3.1.2 Le niveau de protection dans le pays destinataire est-il adéquat ?

Pour pouvoir communiquer des données à l'étranger, il faut que des conditions spéciales soient remplies, en plus des conditions inhérentes à la protection des données qui concernent le devoir général de diligence (ch. 2.1 b). Ces conditions spéciales figurent à l'art. 6 LPD, qui dispose que des données ne peuvent être communiquées à l'étranger que si le pays de destination dispose d'une législation prévoyant un niveau de protection des données adéquat (art. 6, al. 1, LPD) ou, en l'absence d'une telle législation, si le niveau de protection est assuré par d'autres règles ou garanties (art. 6, al. 2, let. a et g, LPD). 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.

En vertu du devoir spécial de diligence prévu à l'art. 6, al. 1, LPD, la communication de données à l'étranger est conforme à la législation sur la protection des données si le pays destinataire dispose d'une législation assurant un niveau de protection adéquat. Le caractère adéquat du niveau de protection doit être examiné à l'aune des prescriptions juridiques de nature générale et sectorielle qui

sont applicables dans l'État considéré. Cet examen doit notamment établir si la législation et la pratique juridique de l'État destinataire tiennent compte des principes inscrits dans la Convention STE 108 et dans son Protocole additionnel. Plus spécialement, il s'agit de déterminer comment la personne concernée peut sauvegarder ses intérêts en cas d'inobservation de ces principes, mais également si le droit d'accès est garanti. Si la législation du pays destinataire n'offre pas un niveau de protection adéquat, les données ne peuvent être communiquées que si les conditions figurant à l'art. 6, al. 2, LPD sont remplies.

Le PFPDT peut aussi déterminer de manière générale si le niveau de protection dans un État est adéquat, de telle sorte que toutes les communications de données vers cet État soient autorisées (art. 31, al. 1, let. d, LPD). Cela présuppose notamment que le destinataire des données soit soumis à une loi qui offre un niveau de protection des données comparable à celui offert par le droit suisse: garantie des droits des personnes concernées (en particulier le droit d'accès [art. 1, al. 6, OLPD] et le droit à l'information [art. 4, al. 4 et 5, LPD]), respect des principes majeurs de protection des données, organe de contrôle indépendant.

L'adéquation du niveau de protection offert par la législation de l'État destinataire est assurée si elle satisfait aux exigences fixées dans la Convention STE 108. Qui plus est, le PFPDT doit aussi tenir compte de la manière dont cette législation est appliquée. Il publie une liste des États qui répondent à ces exigences (art. 7 OLPD).

Cette liste contient, outre les États qui sont parties à la Convention STE 108 et à son Protocole additionnel, les États qui, de l'avis du PFPDT, assurent un niveau de protection adéquat. La personne privée ou l'organe fédéral qui communique des données à quelqu'un se trouvant dans un État figurant sur la liste en question peut partir de l'idée qu'il agit en toute bonne foi. Par contre, s'il sait 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, il n'est plus de bonne foi. En pareil cas, la communication ne doit intervenir qu'aux conditions spécifiées à l'art. 6, al. 2, LPD.

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.

Avec l'application du «Swiss-US- Privacy Shield», suite à l'invalidation de l'accord « Safe Harbor », les États-Unis font à nouveau partie des États garantissant, sous certaines conditions, un niveau adéquat de protection des données au sens de l'art. 6 al.1 LPD. Un niveau de protection adéquat est désormais reconnu pour les entreprises américaines qui adhèrent au Privacy Shield et qui figurent à ce titre sur la liste du Ministère américain du Commerce (US Department of Commerce, DOC) Par rapport à l'accord « Safe Harbor », le Privacy Shield renforce les principes de protection des données et améliore la surveillance exercée par les autorités américaines. Les personnes concernées disposeront, entre autres, d'instruments concrets pour s'informer directement auprès des entreprises certifiées ou des autorités compétentes de l'usage qui est fait de leurs données personnelles, ainsi que pour obtenir la correction ou la suppression de leurs données. Un dispositif de médiation permettra également aux personnes concernées d'influer indirectement sur le traitement des données personnelles effectué par les instances de sécurité américaines. Le PFPDT sert ainsi d'interlocuteur en cas de problèmes relatifs aux données transmises aux États-Unis. Dès que le processus de certification sera activé aux États-Unis et que les informations y relatives seront disponibles, nous insérerons un lien vers la liste de toutes les entreprises américaines certifiées et vers des documents complémentaires.

Si la personne ou l'organe fédéral qui communique des données arrive à la conclusion, dans un cas précis, sur la base de l'examen auquel il a procédé, que le niveau de protection offert par la législation d'un pays considéré est adéquat et que, par ailleurs, les principes généraux de protection des données sont respectés, les données peuvent être communiquées. Par contre, s'il arrive à la conclusion que le niveau de protection n'est pas adéquat dans le pays destinataire, la communication ne peut avoir lieu que si les conditions fixées à l'art. 6, al. 2, LPD sont remplies.

Exemple: si le pays destinataire dispose d'une législation n'offrant un niveau de protection adéquat que pour les données relatives aux personnes physiques, l'art. 6, al. 2, LPD s'applique en cas de communication de données concernant des personnes morales.

3.2 Les modifications de l'art. 6, al. 2, LPD

3.2.1 Remarques générales

Si la personne qui doit communiquer des données arrive à la conclusion que la législation de l'État destinataire n'offre pas un niveau de protection adéquat, les données ne peuvent être communiquées que si l'une des conditions fixées à l'art. 6, al. 2, LPD est remplie. Les let. a et g de l'art. 6, al. 2, permettent la communication à l'étranger uniquement si elle est assurée par des garanties ou des règles de protection des données. 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.

3.2.2 Les conditions alternatives

Art. 6, al. 2, let. a, LPD: la communication des données est justifiée par un contrat

En l'absence de législation assurant un niveau de protection adéquat, la communication de données est licite si d'autres garanties suffisantes existent. Ces garanties peuvent consister en un ensemble de règles que les personnes ou les organes fédéraux échangeant des données s'engagent à respecter. Le PFPDT publie une liste des contrats-modèles ou des clauses standard établis ou reconnus par lui (art. 6, al. 3, dernière phrase, OLPD). Les contrats-modèles existants et reconnus qui régissent la communication de données à l'étranger 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#h2-5;
- 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/ModelContract_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; Ce contrat s'applique exclusivement à la communication de données à l'étranger à des fins d'externalisation (art. 10a LPD). En cas d'externalisation, le but du traitement reste toujours le même tant pour le mandant que pour le mandataire (la gestion des salaires est par exemple confiée à un mandataire à l'étranger). 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 (art. 3, let. i, LPD). 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.[1]

Les personnes ou les organes fédéraux qui échangent des données sont libres d'utiliser d'autres formes de contrat ou de garantie. Ni la forme ni le contenu des clauses contractuelles ne sont définis explicitement dans la LPD; il peut s'agir d'un contrat spécifique relevant de la protection des données ou de clauses de protection des données figurant dans un autre contrat. 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 de données, en particulier l'identité de l'expéditeur et du destinataire des données, les catégories correspondant aux données à communiquer, les buts de la

[1] Modifié en novembre 2010

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, et prévoir un mécanisme de contrôle. Par ailleurs, si la communication porte sur des données sensibles ou des profils de la personnalité, il y a lieu de prévoir par contrat des mesures supplémentaires destinées à garantir la sécurité et la confidentialité.

Le PFPDT doit notamment être informé des garanties visées à l'art. 6, al. 2, let. a, LPD (art. 6, al. 3, LPD et art. 6, al. 1, OLPD). Par la suite, le devoir d'information est considéré comme rempli pour toutes les communications suivantes qui se basent sur les mêmes garanties, pour autant que les catégories de destinataires, les finalités du traitement et les catégories de données à communiquer soient similaires (art. 6, al. 2, let. a, OLPD).

Art. 6, al. 2, let. b, LPD: la communication des données est justifiée par le consentement de la personne concernée

La communication est circonscrite, comme l'indique le libellé de cette disposition, à un cas d'espèce; elle doit concerner un cas particulier, c'est-à-dire une situation concrète. La personne concernée ne peut pas donner son consentement de façon générale et permettre ainsi que l'on communique régulièrement et systématiquement des données la concernant à l'étranger à des fins diverses et dans différentes situations.

Elle peut en revanche, dans un cas concret, donner son consentement à plusieurs communications si les circonstances dans lesquelles elles sont faites restent les mêmes, ce qui signifie que les communications qui sont faites aux mêmes conditions (destinataire, but, transmission éventuelle) peuvent se référer à un seul et même consentement (voir le message relatif à la révision de la LPD, p. 1941). À titre d'exemple, la communication de plusieurs procès-verbaux d'un groupe de travail dont font partie des personnes provenant de différents pays est autorisée sans qu'il faille requérir leur consentement pour la communication de chaque document.

Le consentement doit être donné librement après que la personne a été dûment informée (art. 4, al. 5, LPD). Il doit en outre être explicite si la communication porte sur des données sensibles. La personne concernée doit savoir quelles données la concernant sont communiquées, à quel destinataire et dans quel but. Elle doit aussi être informée si le niveau de protection des données n'est pas adéquat.

La volonté de la personne concernée de consentir à la communication doit être exprimée de façon explicite, et le consentement doit 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.

Art. 6, al. 2, let. c, LPD: la communication des données est justifiée par le besoin de disposer des données pour conclure ou exécuter un contrat

Cette disposition porte sur la communication de données personnelles à des tiers à l'étranger en vue de la conclusion ou de l'exécution d'un contrat. Entrent en ligne de compte avant tout les contrats de prestations de services. Les données à communiquer doivent être celles qui portent sur le partenaire contractuel.

À titre d'exemple, si un contrat incluant la réservation d'un hôtel à l'étranger est conclu avec une agence de voyages, celle-ci est autorisée à communiquer à l'hôtel en question les données concernant la clientèle qui sont nécessaires à l'exécution du contrat.

Voici d'autres exemples de communication de données à des tiers, par l'entremise du partenaire contractuel, dans le cadre de la conclusion ou de l'exécution d'un contrat:

- 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.

En revanche, si l'on veut communiquer des données concernant un tiers qui n'est pas un partenaire contractuel, il faut obtenir son consentement (p. ex. données d'acheminement concernant un tiers en cas d'achats sur Internet). Le consentement n'est par contre pas nécessaire si le tiers entretient des relations contractuelles avec l'un des cocontractants (p. ex. en qualité de mandataire). Si le tiers est le bénéficiaire de la prestation contractuelle, on part souvent de l'idée que le consentement est tacite.

Art. 6, al. 2, let. d, LPD: la communication des données est justifiée par des intérêts publics prépondérants ou par des exigences inhérentes à une procédure judiciaire

La communication de données en vertu de cette disposition présuppose qu'elle est justifiée par un intérêt public prépondérant ou par des exigences inhérentes à une procédure judiciaire. Un intérêt public prépondérant ne doit pas forcément être un intérêt suisse, mais il doit être examiné à la lumière du droit suisse. On est en présence d'un tel intérêt par exemple lorsque, pour des raisons de sécurité, une équipe 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 contre, 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).

La communication de données n'est possible qu'en l'espèce, c'est-à-dire dans une situation bien précise ou dans un cas concret. Elle doit être indispensable à la sauvegarde de l'intérêt qui est invoqué. Les communications de données systématiques ou régulières ne sont pas couvertes.

Les données à communiquer peuvent concerner aussi bien une que plusieurs personnes.

La personne qui va transmettre les données doit examiner s'il existe un intérêt prépondérant en tenant compte de toutes les circonstances. Elle doit notamment déterminer si l'État destinataire pourrait transmettre ces données à des tiers sans garantir un niveau de protection des données adéquat.

D'autres intérêts prépondérants, publics ou privés, peuvent empêcher la communication des données.

En vertu de cette disposition, il est aussi possible de communiquer des données à l'étranger pour constater, exercer ou défendre un droit en justice. La disposition permet à une personne de communiquer des données concernant un tiers à une autorité judiciaire ou arbitrale sans qu'un niveau de protection des données adéquat soit garanti si elle veut faire valoir des prétentions juridiques contre le tiers en question. Il peut s'agir en l'occurrence d'une procédure relevant du droit civil, pénal ou administratif. Les données doivent toutefois être indispensables au but recherché et, en plus, avoir un lien étroit avec la procédure. Cela signifie que la communication doit être précédée d'une pesée des intérêts. S'il est possible de faire valoir les prétentions juridiques sans que la communication des données ait lieu, l'intérêt de la personne concernée à voir garantie la protection des données la concernant doit l'emporter. Si, par exemple, il existe des doutes sur le respect du principe de finalité par l'autorité judiciaire étrangère, il faut renoncer à la communication des données. La personne qui communique les données peut se faire confirmer ce respect. Il est aussi possible d'effectuer la communication des données en dehors d'une procédure judiciaire, notamment pour faire en sorte qu'un avocat à l'étranger détermine l'opportunité d'une telle procédure.

La personne communiquant les données ne doit pas obligatoirement être partie à la procédure. Il peut aussi s'agir d'un organe public, d'un expert ou d'un témoin.

Un organe fédéral peut communiquer des données pour permettre à une personne de faire valoir des prétentions juridiques à l'égard d'un tiers (art. 19, al. 1, let. d, LPD).

Art. 6, al. 2, let. e, LPD: la communication des données est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée

Une communication n'est licite en vertu de cette disposition que si elle a pour but de protéger des intérêts vitaux de la personne concernée et que si cette dernière n'est pas en mesure de faire valoir ses propres intérêts (par exemple à la suite d'un accident survenu à l'étranger). Il doit aller de soi que cette personne aurait donné son consentement à une telle communication.

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.

Art. 6, al. 2, let. f, LPD: la communication des données est justifiée par leur mise à disposition à tout un chacun par la personne concernée

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 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).

Art. 6, al. 2, let. g, LPD: la communication des données est justifiée par des règles de protection des données internes à un groupe de sociétés

Cette disposition permet la communication transfrontière de données au sein d'un groupe de sociétés, la définition du terme de «groupe de sociétés» étant celle qui figure à l'art. 663e, al. 1, CO (RS 220). En vertu de cette disposition de la LPD, la société n'est pas libérée de l'obligation, pour les traitements de données effectués en Suisse, consistant à respecter les autres dispositions de la LPD, notamment celles qui régissent l'information des personnes concernées et le droit d'accès.

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 PFPDT doit être informé des règles édictées (art. 6, al. 3, LPD).

L'aspect formel du caractère contraignant peut être conféré par exemple par une décision du conseil d'administration. Les différentes sociétés doivent reprendre et appliquer les règles. L'application pratique peut être garantie par exemple par des audits.

Le droit suisse ne prévoit aucune approbation des règles de protection des données par le PFPDT. Ce dernier doit simplement être informé. Les modifications et les adaptations de ces règles peuvent être opérées dans certaines limites sans qu'il faille procéder à une nouvelle information.

Le PFPDT doit être informé notamment des garanties visées à l'al. 2, let. g, LPD (voir aussi l'art. 6, al. 3, LPD). S'il a été informé des règles de protection des données, 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 (art. 6, al. 2, let. a, OLPD).

3.3 Les modifications de l'art. 6, al. 3, LPD

3.3.1 Remarques générales

Le devoir d'information incombant au maître d'un fichier

Le maître d'un fichier doit informer le PFPDT dans les cas où la protection des données va être garantie par un contrat (art. 6, al. 2, let. a, LPD) ou par d'autres règles de protection des données (art. 6, al. 2, let. g, LPD; voir aussi l'art. 6, al. 1, OLPD). L'information va ainsi porter sur les garanties et les règles de protection des données, et non pas sur la communication des données en tant que telle. Le maître du fichier informe le PFPDT si possible avant la communication des données à l'étranger. L'article ne fixe aucun délai précis; il accorde une certaine souplesse au maître du fichier. Si ce dernier n'est pas en mesure d'informer le PFPDT avant la communication, il doit le faire dès que possible. Après la première information, le devoir d'information est considéré comme rempli pour toutes les communications suivantes qui se basent sur les mêmes garanties, pour autant que les catégories de destinataires, les finalités du traitement et les catégories de données à communiquer soient similaires. En cas de transfert de données entre des sociétés faisant partie d'un même groupe, une seule et unique information sur les règles de protection des données que doivent appliquer les sociétés concernées suffit également. 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).

L'information consiste à envoyer au PFPDT un exemplaire ou une copie des garanties convenues avec le destinataire ou des règles de protection des données en vigueur dans la société concernée.

L'art. 6, al. 3, OLPD prévoit une sorte de devoir d'information simplifié dans les cas où le maître d'un fichier utilise des contrats-types ou des clauses contractuelles standard qui ont été établis ou reconnus par le PFPDT (voir la liste figurant dans le commentaire de l'art. 6, al. 2, let. a, LPD au ch. 3.2.2). Dans un tel cas de figure, le maître du fichier doit simplement informer le PFPDT, sans entrer dans les détails, du fait qu'il utilise généralement les contrats-types ou les clauses contractuelles standard reconnus par le PFPDT pour communiquer des données dans des États qui ne disposent pas d'une législation sur la protection des données offrant un niveau de protection adéquat. Il n'a pas besoin de lui envoyer un exemplaire ou une copie.

Si le maître du fichier utilise toutefois d'autres garanties dans certains cas ou pour certaines parties de la communication des données, il doit en informer le PFPDT selon la procédure ordinaire.

Le devoir d'examen incombant au PFPDT

L'information doit permettre au PFPDT d'examiner si les mesures de protection ou les règles de protection des données visées à l'art. 6, al. 2, let. a et g, LPD sont adéquates. Le PFPDT a un devoir d'examen (art. 31 al. 1, let. e, LPD). En cas d'information ordinaire (voir le ch. 3.3.1 a), le PFPDT examine l'ensemble du dispositif réglementaire. Par contre, en cas d'information simplifiée, il examine uniquement les buts de la communication de données ainsi que son opportunité et sa proportionnalité. Il n'examine pas les différentes dispositions du dispositif réglementaire standard utilisé.

L'art. 6, al. 5, OLPD dispose que le PFPDT a 30 jours pour examiner si les garanties et les règles qu'on lui a communiquées assurent un niveau de protection des données adéquat. Si tel n'est pas le cas, le PFPDT prend contact avec le maître du fichier et édicte au besoin 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.

4. responsabilité et prétentions

4.1 Responsabilité du maître du fichier en cas de violation du devoir de diligence

Le maître du fichier répond des préjudices que pourrait causer 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).

4.2 Prétentions de la personne concernée en cas de violation du devoir de diligence

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