ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08, F +41 26 305 59 72
www.fr.ch/atprd

COMMUNICATION TRANSFRONTIÈRE

Feuille informative concernant les communications transfrontières

1. Objectif

La présente Feuille informative se fonde sur le pouvoir de conseil de la Préposée (art. 31 al. 2 let. b de la Loi du 25 novembre 1994 sur la protection des données, LPrD). Elle a pour but d'aider les organes publics à suivre la procédure adéquate lors de demandes de communications transfrontières de données personnelles (art. 12a LPrD).

2. Généralités

2.1 Mise en conformité avec la législation européenne

Les autorités européennes ont élaboré des instruments juridiques visant à harmoniser la protection des données au niveau international et à définir un standard minimal de protection qui doit être garanti dans tous les Etats membres. Il s'agit principalement de la *Convention du 28 janvier 1981 du Conseil de l'Europe* pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (convention STE 108), de son *Protocole additionnel du 8 novembre 2001* concernant les autorités de contrôle et les flux transfrontières de données et de la *Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil (UE),* relative à la protection des données à caractère personnel et la libre circulation de ces données. Ces règles ont été transposées dans la législation suisse, y compris au niveau cantonal.

2.2 Notion

La disposition de la LPrD concernant les flux transfrontières est la suivante.

Art. 12a Communication transfrontière

1 Des données personnelles ne peuvent être communiquées à l'étranger que dans les Etats qui garantissent un niveau de protection adéquat.

2 Des données personnelles peuvent toutefois être communiquées dans les Etats n'offrant pas une telle garantie, lorsque l'une des conditions suivantes est réalisée :

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 explicite;

c) le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat, et les données traitées concernent le cocontractant ou la cocontractante;

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 à la protection de la vie ou de l'intégrité corporelle de la personne concernée.

3 L'organe public informe le ou la préposé-e cantonal-e à la protection des données des garanties prises en vertu de l'alinéa 2 let. a avant la communication des données à l'étranger.

Cette disposition ne donnant pas de définition, nous nous référons à celle qui figure sur le site du Préposé fédéral à la protection des données et à la transparence (PFPDT). Il y a une « *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.* » (Explications relatives à la communication de données personnelles à l'étranger, 2.1.1.p. 3).

http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=fr

A relever ici que, lors de l'examen sur l'admissibilité de la transmission de données personnelles à l'étranger, l'organe public concerné doit vérifier en premier lieu que la **législation cantonale le permet** (phase 1), puis, en deuxième lieu que les données personnelles transmises seront soumises à une **législation de l'Etat étranger assurant un niveau de protection adéquat** (phase 2). La présente Feuille informative s'attache principalement à la phase 2.

3. Evaluation du niveau de protection adéquat

3.1 Liste des Etats

Selon l'art. 12a al. 1 LPrD, *« des données personnelles ne peuvent être communiquées à l'étranger que dans les Etats qui garantissent un niveau de protection adéquat. »*. La problématique réside dans le fait d'évaluer le niveau de protection adéquat. Le PFPDT a établi une **liste des Etats ayant un niveau de protection adéquat** (la liste est accessible sur le site du PFPDT sous http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=fr

3.2 Inscription dans la liste

Pour inscrire un Etat sur cette liste et pour permettre que toutes les communications de données vers cet Etat destinataire soient autorisées, le PFPDT vérifie que **sa législation et sa pratique juridique tiennent compte des principes inscrits dans la Convention STE 108 et dans son Protocole additionnel**. En effet, il faut qu'il dispose d'une loi qui offre un niveau de protection des données comparable à celui offert par le droit suisse (garantie des droits des personnes concernées, respect des principes majeurs de protection des données, organe de contrôle indépendant) et qu'en plus, il l'applique de manière correcte. En particulier, il s'agit de déterminer comment la personne concernée peut sauvegarder ses intérêts en cas d'inobservation de ces principes et si le droit d'accès aux données personnelles la concernant est garanti.

3.3 Vérification par l'organe public de la présence sur la liste

Dès lors, l'organe public doit d'abord **vérifier la présence de l'Etat destinataire sur la liste du PFPDT**. Celle-ci est régulièrement actualisée. Toutefois, si un Etat n'y figure pas, cela ne veut pas forcément dire qu'il ne dispose pas d'une législation sur la protection des données assurant un niveau de protection adéquat. Néanmoins, l'Autorité cantonale de surveillance en matière de protection des données se fonde normalement sur la liste d'Etats citée, sous réserve de vérifications nécessaires.

3.4 Autres exigences pour l'organe public

Bien que l'organe public qui communique des données à un autre se trouvant dans un de ces Etats puisse partir de l'idée qu'il agit de bonne foi, le fait qu'un Etat figure sur la liste ne donne pas toute liberté de communiquer des données personnelles électroniques. L'organe public qui traite des données personnelles est responsable de la protection des données au sens de l'art. 17 LPrD. Il doit notamment **s'assurer** que la communication repose sur des **bases légales**, que le mode de communication dans le cas d'espèce est suffisamment **sécurisé** au sens des dispositions légales (art. 22 LPrD, Règlement du 29 juin 1999 sur la sécurité des données personnelles, RSD) et que les données sont **parvenues au bon destinataire**. Par conséquent, s'il ne prouve pas qu'il a pris toutes les mesures nécessaires pour assurer un niveau de protection adéquat, il sera responsable, et d'autant plus si la communication porte sur des données sensibles (devoir de diligence accru, art. 17 et 8 LPrD).

4. Le cas d'un Etat qui ne figure pas sur la liste

4.1 Préliminaire

Si l'Etat destinataire ne figure pas sur la liste, il est cependant possible dans certains cas de communiquer des données. L'art. 12a al. 2 prévoit des conditions qui sont en grande partie identiques à celles de la législation fédérale. Le Message no 56 du Conseil d'Etat accompagnant le projet de modification de la LPrD énonce que *« les exceptions prévues par le droit cantonal doivent être interprétées de la même manière que celles qui sont applicables au niveau fédéral »* (p. 661). http://admin.fr.ch/fr/data/pdf/gc/2007_11/bgc/56_message_f.pdf. Dès lors, nous reprenons les indications du PFPDT que l'on trouve à l'adresse suivante : http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=fr.

4.2 Conditions de communication admissible (alternatives, art. 12a al. 2 LPrD)

L'art. 12a al. 2 LPrD prévoit que *« des données personnelles peuvent toutefois être communiquées dans les Etats n'offrant pas une telle garantie, lorsque **l'une des conditions suivantes** est réalisée »*.

4.2.1 «a) *Des garanties suffisantes, notamment **contractuelles**, permettent d'assurer un niveau de protection adéquat à l'étranger »*.

Voici des **exemples de contrats** admissibles (se référer à l'adresse du PFPDT ci-dessus) :

- *clauses contractuelles types de l'Union européenne* :
- *des contrats-type du Conseil de l'Europe* qui visent à assurer une protection équivalente des données dans le cadre des flux transfrontières de données
- *contrats-type* pour l'externalisation du traitement de données à l'étranger
- *Safe Harbor Agreement* qui est un accord entre la Commission européenne et les Etats-Unis. En vertu de cet accord, l'organisation américaine destinataire de la communication de données provenant de Suisse peut en plus s'engager par écrit à appliquer les mêmes règles de protection de données que pour les données provenant d'un Etat membre de l'UE.

Les personnes ou les organes publics qui veulent communiquer des données peuvent aussi utiliser **d'autres formes de contrat ou de garantie**, par ex. un contrat spécifique de protection des données ou des clauses de protection des données figurant dans d'autres contrats. Mais ils doivent garantir un niveau de protection adéquat, c'est-à-dire conforme à la LPrD et englober les 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 engagements contractuels **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.

Pour les cas de communications de données personnelles fondés sur un contrat de mandat, se référer également à l'Aide-mémoire no 5 Mandat (outsourcing) http://appl.fr.ch/sprd/pour_en_savoir_plus/Outsourcing/no5_aidememoire_outsourcing_fr.pdf.

4.2.2 *«b) La personne concernée a, en l'espèce, donné son **consentement explicite**»*

Ce motif est en aucun cas, à traiter de façon générale mais toujours individuellement, pour chaque communication. En effet, consentir de façon générale à la communication régulière et systématique de données à l'étranger à des fins diverses et dans différentes situations n'est pas admissible. A 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. Le consentement ne libère pas le responsable 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. Il doit en particulier :

- être donné librement;
- être donné après que la personne concernée a été dûment informée ;
- être explicite si la communication porte sur des données sensibles;
- pouvoir être retiré à tout moment pour de futurs traitements ou communications de données.

4.2.3 *«c) Le traitement est en relation directe avec **la conclusion ou l'exécution d'un contrat**, et les données traitées concernent le cocontractant ou la cocontractante»*

Ce sera par ex. le cas :

- de l'organe public qui souhaite communiquer des données de collaborateurs-trices à un hôtel à l'étranger dans le cadre d'un congrès;
- d'un organe public qui veut transmettre des données dans le cadre de transactions bancaires ou de mandats relevant du trafic des paiements à l'échelle internationale.

4.2.4 *« 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**»*

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.

4.2.5 *« e) La communication est, en l'espèce, nécessaire à la **protection de la vie ou de l'intégrité corporelle** de la personne concernée. »*

Ce sera par ex. le cas lorsque :

- des intérêts vitaux de la personne concernée sont en jeu;
- la personne concernée n'est pas en mesure de faire valoir ses propres intérêts (par ex, à la suite d'un accident survenu à l'étranger);
- une présomption est admissible que la personne concernée va donner son consentement à la communication des données ;
- des données concernant des proches de la personne concernée pourront 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.

5. Information préalable à la Préposée (art. 12a al. 3 LPrD)

5.1 Principe

En vertu de l'art. 12a al. 3 LPrD, *« l'organe public informe le ou la préposé-e cantonal-e à la protection des données des garanties prises en vertu de l'alinéa 2 let. a avant la communication des données à l'étranger. »*

Il y a donc lieu d'informer la Préposée à la protection des données au moment des garanties de la protection des données dans un contrat.

5.2 Comment la Préposée doit-elle être informée?

- 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 responsable du fichier en *informe* la Préposée de cette utilisation, sans entrer dans les détails. Si le responsable du fichier utilise *d'autres garanties* dans certains cas ou pour certaines parties de la communication des données, il en informe la Préposée 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.
- La Préposée *ne doit pas être informée* 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 responsable du fichier informe la Préposée *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.

5.3 En quoi consiste l'examen effectué par la Préposée ?

- En cas d'utilisation de contrats-types reconnus pour la communication de données à l'étranger, la Préposée n'effectue *aucun examen du dispositif réglementaire*; elle 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, la Préposée peut examiner le dispositif réglementaire. Si les garanties et les règles n'assurent pas un niveau de protection des données adéquat, la Préposée peut prendre contact avec le responsable du fichier et, si nécessaire, suggérer des modifications.

6. Moyens à disposition de l'Autorité en cas de garantie insuffisante

Dans le cas où la Préposée jugerait les garanties insuffisantes et que l'organe public ne se conforme pas à ses suggestions, elle ne pourrait pas s'opposer à la communication de données à l'étranger par l'organe public concerné qui applique la procédure prévue à l'art. 12a al. 3 LPrD. Dans ce cas, seule la Commission cantonale de la protection des données dispose des moyens octroyés par l'art. 22a LPrD. Elle peut ainsi formuler une *recommandation de renoncer à la*

communication à l'encontre de l'organe public et pourra *recourir* auprès du Tribunal cantonal contre une décision négative de l'organe public (art. 27 LPrD).

Quant à la personne qui s'estime lésée, elle dispose des moyens légaux prévus aux art. 26 ss. LPrD (droits en cas d'atteinte et réparation du dommage et du tort moral).

7. Mise en œuvre

En résumé, voici les principales tâches de l'organe public :

1. Vérifier que la communication repose sur des bases légales cantonales suffisantes (art. 4 et 10 LPrD).
2. S'assurer que les conditions légales cantonales à la communication sont remplies (notamment en matière de sécurité, art. 22 LPrD et dispositions réglementaires y relatives).
3. Vérifier que l'Etat destinataire, à qui il veut communiquer des données, figure sur la liste agréée en vertu de l'art. 12a al. 1 LPrD.
4. Si l'Etat n'y figure pas, examiner si une des conditions particulières de l'art. 12a al. 2 LPrD est remplie.
5. En cas de garantie contractuelle selon l'art. 12a al. 2 let. a LPrD, informer la Préposée préalablement au transfert des données (art. 12a al. 3LPrD), aussi lors de nouvelles demandes de communications transfrontières.

Annexe

COMMUNICATION TRANSFRONTIERE

Références

Textes légaux

- Loi du 25 novembre 1994 sur la protection des données (LPrD)
- Règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD)
- Loi fédérale du 19 juin 1992 sur la protection des données (LPD)
- Ordonnance du 14 juin 1993 relative à la Loi fédérale sur la protection des données (OLPD)

Documents

- La Communication de données à l'étranger en 24 questions
- Explications relatives à la communication de données personnelles à l'étranger suite à la révision de la loi fédérale sur la protection des données
- Guide pour le traitement des données personnelles dans le secteur privé (pp 7-8)
- Communication de données à des autorités étrangères

Tous les documents ci-dessus sont disponibles sur le site du Préposé fédéral, à l'adresse suivante :

http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=fr

- Message n°56 du Conseil d'Etat au Grand Conseil accompagnant le projet de loi modifiant la loi sur la protection des données (adaptation au droit international, en particulier aux accords Schengen/Dublin) http://admin.fr.ch/fr/data/pdf/gc/2007_11/bgc/56_message_f.pdf