ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence, de la protection des données et de la médiation ATPrDM
Kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation ÖDSMB

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08
www.fr.ch/atprdm
Réf : 2023-PrD-200

COMMUNICATION TRANSFRONTIÈRE

Feuille informative concernant les communications transfrontières

I. Généralités

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 États 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 108+), de son Protocole additionnel du 8 novembre 2001 concernant les autorités de contrôle et les flux transfrontières de données. Ces règles ont été transposées dans la législation suisse, y compris au niveau cantonal.

La présente Feuille informative se fonde sur le pouvoir de conseil du ou de la préposé-e (art. 54 al. 1 let. d et j de la loi du 12 octobre 2023 sur la protection des données ; ci-après : LPrD ; RSF 17.1). Elle a pour but d'aider les organes publics à suivre la procédure adéquate lors de demandes de communications transfrontières de données personnelles (art. 15 LPrD).

Cette fiche vise donc à présenter la notion de flux transfrontière, à préciser ses bases légales mais surtout à concrètement expliquer le déroulement d'une communication transfrontière afin qu'un organe public puisse si besoin réaliser en pratique une telle communication de données.

II. Notion

Par flux transfrontière, on entend *toute communication de données personnelles vers un État étranger ou un organisme international*. La communication consiste à rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant, en les diffusant ou en les publiant.

III. Bases légales

À titre liminaire, il convient de rappeler que *les conditions générales* pour une communication de données personnelles sont énumérées par l'article 14 LPrD. Ces conditions doivent également être respectées dans le cadre d'une communication transfrontière.

L'article 15 LPrD précise quant à lui les *exigences supplémentaires* qui doivent être remplies pour le cas particulier de la communication transfrontière de données d'une personne physique.

Art. 15 Communication – Conditions supplémentaires pour les communications transfrontière

[1] Les **données personnelles** d'une **personne physique** peuvent être communiquées **vers un État étranger ou vers un organisme international** dans la mesure où il existe **une décision du Conseil fédéral** attestant que l'État ou l'organisme international destinataire des données garantit un niveau de protection adéquat.

[2] En l'absence d'une telle décision, la communication ne peut avoir lieu que si :

a) des garanties suffisantes, notamment contractuelles, conventionnelles, techniques et/ou organisationnelles, permettent d'assurer un niveau de protection adéquat à l'étranger ;
b) 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 ;
c) la personne concernée a, en l'espèce, donné son consentement explicite à la communication ;
d) le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat, et les données traitées concernent une partie au contrat ;
e) la communication est, en l'espèce, nécessaire à la protection de la vie ou de l'intégrité corporelle de la personne concernée ou d'un tiers.

[3] Avant la communication des données personnelles à l'étranger, le ou la préposé-e à la transparence et à la protection des données (ci-après : le ou la préposé-e) est informé-e à temps des garanties prévues à l'alinéa 2 lettre a. Sur demande, il ou elle peut en tout temps obtenir des informations visant à vérifier qu'une communication de données à l'étranger répond aux exigences formulées aux lettres b à e.

[4] Ne sont pas considérées comme faisant l'objet d'une communication à l'étranger les données qui sont simplement publiées au moyen d'un site Internet ouvert au public.

IV. Données concernées

Pour rappel, la LPrD régit la protection de données personnelles. Sont des données personnelles *toutes les informations qui se rapportent à une personne identifiée ou identifiables* (art. 4 al. 1 let. a LPrD).

Les règles spéciales de l'article 15 LPrD ne s'appliquent cependant qu'à la communication de *données personnelles se rapportant à des personnes physiques*. La communication transfrontière de données personnelles de personnes morales ne sont pas soumises à ces exigences supplémentaires.

V. Mise en œuvre pratique de la communication transfrontière

A. L'analyse des conditions légales appliquées dans un cas d'espèce

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 qu'il existe *une décision du Conseil fédéral* attestant que l'État ou l'organisme international destinataire des données garantit un niveau de protection adéquat.

Ainsi, il découle de cette disposition deux hypothèses, selon que l'État destinataire fait ou ne fait pas l'objet d'une décision du Conseil fédéral attestant que celui-ci garantit un niveau de protection adéquat.

1. Première hypothèse : l'État destinataire est reconnu comme offrant un niveau de protection adéquat et figure ainsi sur la liste dressée par le Conseil fédéral

Dans un tel cas, l'organe public peut communiquer les données personnelles d'une personne physique vers l'État ou l'organisme international car le Conseil fédéral a rendu une décision par laquelle il reconnaît qu'il existe un niveau de protection des données équivalent à celui de la Suisse.

La liste officielle est celle publiée dans l'annexe 1 de l'Ordonnance sur la protection des données du 31 août 2022 (RS 235.11)[1].

Ainsi, l'organe public qui communique des données à un autre se trouvant dans un de ces États peut partir de l'idée qu'il agit de bonne foi. Toutefois, il convient de relever qu'il *reste responsable de la protection des données* au sens de l'article 36 alinéa 1 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. 40 LPrD ; cf. ég. le règlement du 29 juin 1999 sur la sécurité des données personnelles ; ci-après : RSD ; RSF 17.15) 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 engage sa responsabilité (art. 35 al. 1 LPrD), et d'autant plus si la communication porte sur des données sensibles, lesquelles obligent le responsable de traitement à faire preuve d'un devoir de diligence accrue (art. 36 et 11 LPrD).

[1] Lien : https://www.fedlex.admin.ch/eli/cc/2022/568/fr

2. Deuxième hypothèse : l'État destinataire n'est pas reconnu comme offrant un niveau de protection adéquat et ne figure donc pas sur la liste dressée par le Conseil fédéral

Dans le cas où la communication de données doit s'effectuer à destination d'un État ne figurant pas dans la liste du Conseil fédéral, l'organe public responsable doit veiller au respect des conditions prévues à l'article 15 LPrD, qui sont en grande partie inspirées celles de la législation fédérale.

Le Message 2023-CE-149 du Conseil d'État du 26 juin 2023 accompagnant le projet de modification de la LPrD indique que « lorsque le pays destinataire est un pays tiers qui n'offre pas un niveau de protection adéquat ou en cas de doute à ce sujet, une communication de données transfrontière reste malgré tout possible en présence d'autres garanties suffisantes ou s'il existe un motif justificatif à la communication (al. 2). Par rapport à l'avant-projet et à la loi actuelle, la liste des garanties suffisantes a été précisée par la mention *des mesures techniques et/ou organisationnelles en plus des mesures contractuelles*. En pratique, il peut s'avérer nécessaire suivant les cas de *cumuler plusieurs types de mesures entre elles* » (p. 20).

a. En cas de garanties suffisantes

En premier lieu, l'organe public peut demander au destinataire de fournir *des garanties suffisantes, notamment contractuelles, conventionnelles, techniques et/ou organisationnelles permettant d'assurer un niveau de protection adéquat à l'étranger*. Il peut utiliser les clauses contractuelles standards pour le transfert de données personnelles entre l'Union européenne et les pays tiers (Standard contractual clauses for data transfers between EU and non-EU countries[2]), étant précisé que ces clauses ne remplacent pas les conditions et les responsabilités prévues dans la LPrD. Les personnes ou les organes publics 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 autres formes de contrat ou de garantie doivent assurer un niveau de protection adéquat, c'est-à-dire une protection 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 ; et
- 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 ; et
- prévoir des mesures destinées à garantir la sécurité et la confidentialité lors de la communication de données sensibles ou de profils de la personnalité.

[2] Lien : https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

b. En cas de communication indispensable

La communication de données personnelles à destination d'un pays n'étant pas au bénéfice d'une reconnaissance du Conseil fédéral est également possible lorsqu'elle 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 cette hypothèse, 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 ; et
- intervenir dans un cas concret, c'est-à-dire dans une situation précise.

c. En cas de consentement explicite de la personne concernée

Lorsque la personne concernée a, en l'espèce, *donné son consentement explicite à la communication*, celle-ci est admissible.

Ce motif n'est en aucun cas, à considérer 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 licite. 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. 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.

Le consentement de la personne concernée n'est valable qu'aux conditions suivantes :

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

d. En cas de traitement en relation directe avec la conclusion ou l'exécution d'un contrat

Lorsque le traitement est en relation directe avec *la conclusion ou l'exécution d'un contrat*, et les données traitées concernent une partie au contrat, la communication transfrontière avec un pays ne figurant pas dans la liste du Conseil fédéral est licite.

Cette hypothèse vise par exemple les situations suivantes :

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

e. En cas de protection de la vie ou de l'intégrité corporelle d'un tiers

La communication est, en l'espèce, *nécessaire à la protection de la vie ou de l'intégrité corporelle de la personne concernée ou d'un tiers*.

Cette hypothèse vise par exemple les situations suivantes :

- 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 exemple, à la suite d'un accident survenu à l'étranger) ;
- une présomption 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.

B. L'information obligatoire au ou à la préposé-e avant toute communication transfrontière

1. Principe

Comme expliqué précédemment, lorsque la communication transfrontière doit s'effectuer avec un État non reconnu offrir un niveau de protection adéquat, l'organe public doit *prendre des mesures ou invoquer un motif justificatif* (art. 15 al. 2 LPrD).

Parmi les mesures, il peut conclure un contrat visant à obtenir *des garanties suffisantes* pour assurer un niveau de protection adéquat (art. 15 al. 2 let. a LPrD).

Uniquement dans cette situation, avant de procéder à la communication à l'étranger des données personnelles, l*'organe public doit informer le ou la préposé-e des garanties convenues* (art. 15 al. 3 LPrD).

Conformément à l'article 15 alinéa 3 LPrD, avant la communication des données personnelles à l'étranger, le ou la préposé-e est informé-e à temps des garanties prévues à l'article 15 alinéa 2 lettre a. Sur demande, il ou elle peut en tout temps obtenir des informations visant à vérifier qu'une communication de données à l'étranger répond aux exigences formulées aux lettres b à e.

2. Communication de l'information

Le responsable du traitement informe le ou la préposé-e *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 consiste en l'envoi au ou à la préposé-e d'une copie des garanties ou des règles de protection des données convenues avec le destinataire.

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 ou la préposé-e 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.

3. Examen du ou de la préposé-e

En cas d'utilisation de contrats-types reconnus pour la communication de données à l'étranger, le ou la préposé-e n'effectue aucun examen du dispositif réglementaire ; il ou 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, le ou la préposée pourra examiner le dispositif réglementaire. Si les garanties et les règles n'assurent pas un niveau de protection des données adéquat, le ou la préposé-e peut prendre contact avec le responsable du traitement et lui demander de procéder à des adaptations.

4. Moyens à disposition du ou de la préposé-e

Dans le cas où le ou la préposé-e jugerait les garanties insuffisantes et où l'organe public ne se conforme pas à ses observations, le ou la préposé-e pourra rendre une recommandation comme le prévoit l'article 57 LPrD.

Dans le cas où l'organe public ne suit pas la recommandation, le ou la préposé-e pourra transmettre l'affaire à la Commission cantonale de la transparence, de la protection des données et de la médiation (ci-après : la Commission) qui prendra une décision administrative contraignante (art. 57 al. 4 et 58 LPrD).

Dans des cas d'urgence, la Commission peut ordonner des mesures provisionnelles.

Quant à la personne qui s'estime lésée, elle dispose des moyens légaux prévus aux articles 33 à 35 LPrD.

C. Conclusion

La communication transfrontière de données personnelles est une opération sensible qui doit être réalisée dans le respect des règles en vigueur. Il est important de bien analyser la situation au cas par cas afin de déterminer si la communication est licite et de prendre les mesures nécessaires pour protéger les données personnelles.

En principe, les données personnelles ne peuvent être communiquées à un pays étranger que si celui-ci garantit un niveau de protection adéquat. Un tel niveau existe si le Conseil fédéral l'a reconnu à travers une décision.

En l'absence de décision du Conseil fédéral, la communication transfrontière de données est possible si :

- le destinataire des données a fourni des garanties suffisantes pour assurer un niveau de protection adéquat ;
- la communication est indispensable à la sauvegarde d'un intérêt public prépondérant ou à la constatation, l'exercice ou la défense d'un droit en justice ;
- la personne concernée a donné son consentement explicite ;
- le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat ; ou
- la communication est nécessaire à la protection de la vie ou de l'intégrité corporelle de la personne concernée ou d'un tiers.

Dans tous les cas, l'organe public qui souhaite communiquer des données personnelles à destination d'un État non reconnu par une décision du Conseil fédéral doit informer le ou la

préposé-e à la protection des données lorsque cette communication se fonde sur le fait que le destinataire a fourni des garanties suffisantes pour assurer un niveau de protection adéquat. Lorsque cette communication est justifiée pour les autres raisons, le ou la préposé-e à la protection des données peut obtenir les informations pour vérifier que la communication est conforme aux conditions légales.