Le transfert de données à l'étranger : état des lieux en Suisse

Jeremy Reichlin et Livio di Tria, le 18 décembre 2022

Dans le courant de l'été 2021, le PFPDT a publié deux importantes notices relatives au transfert de données dans un pays ne présentant pas le niveau de protection des données requis. Ces publications du PFPDT s'inscrivent en marge de sa décision de reconnaître en Suisse (sous réserve de quelques modifications et compléments) les nouvelles clauses contractuelles types adoptées par la Commission européenne du 4 juin 2021. Le présent article se propose de faire un tour d'horizon du sujet en Suisse un peu plus d'une année après la publication de ces deux notices.

Guide pour l'examen de la licéité de la communication transfrontière de données et Transfert de données personnelles dans un pays ne présentant pas le niveau de protection requis.

Transmission de données d'un responsable de traitement ou sous-traitant à un autre responsable de traitement ou sous-traitant

L'art. 6 LPD précise qu'aucune donnée personnelle ne peut être « communiquée » à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée. Toutefois, ni la loi ni son ordonnance d'exécution ne précisent ce qu'il convient d'entendre par « communication » de données.

Le 18 novembre 2021, le CEPD a publié des lignes directrices concernant l'application du chapitre 5 du RGPD consacré au transfert international de données. Dans ce contexte, le CEPD a précisé que pour qu'il y ait un transfert de données, il faut que l'exportateur de données (soit un responsable du traitement ou un sous-traitant) divulgue par transmission ou par tout autre moyen des données à « un autre responsable du traitement ou à un sous-traitant ».

En d'autres termes, les dispositions sur le transfert de données international ne s'appliquent pas en cas de transfert entre un responsable de traitement ou un sous-traitant et une personne n'agissant pas comme responsable de traitement ou sous-traitant. Tel est notamment le cas lorsque l'employé se connecte depuis l'étranger à sa boîte électronique et consulte des données personnelles dans le cadre de son activité professionnelle.

À notre sens, ces considérations s'appliquent *mutatis mutandis* au transfert de données régi par l'art. 6 LPD, respectivement par l'art. 16 nLPD dès le 1er septembre 2023.

Marche à suivre en cas de transfert de données à l'étranger

Il découle des notices publiées par le PFPDT qu'un transfert de données de la Suisse à l'étranger doit s'effectuer selon les étapes suivantes :

I. Vérification du niveau de protection des données dans le pays de destination

Dans un premier temps, l'exportateur doit déterminer si l'État dans lequel les données doivent être exportées figure sur la liste d'États établie par le PFPDT (ou par le Conseil fédéral selon la nLPD). Même si tel est le cas, l'exportateur doit ensuite vérifier périodiquement si le niveau de protection est toujours adéquat et s'il n'y a pas d'autres raisons s'opposant à un traitement sûr des données personnelles dans le pays de destination.

Le PFPDT précise que l'exportateur qui transfère des données vers un pays figurant sur la liste est présumé être de bonne foi, mais que cette présomption est réfragable. À notre sens, tel pourrait notamment être le cas si un exportateur communique à l'étranger, y compris au sein de l'Union européenne, des données relatives à des personnes morales (qui sont encore protégées jusqu'à l'entrée en force de la nLPD). En effet, compte tenu du fait que le RGPD ne protège pas les données de personnes morales, le niveau de protection des données – pour ce type spécifique de données – n'est pas adéquat et leur communication nécessiterait des mesures de protection additionnelles.

II. Examens des garanties suffisantes en cas d'absence de niveau de protection des données dans le pays de destination

Si, après vérification, il est constaté que le niveau de protection des données dans le pays de destination n'est pas adéquat, l'exportateur doit assurer la protection des données en fournissant des garanties suffisantes, soit dans l'écrasante majorité des cas les nouvelles clauses contractuelles types adoptées par la Commission européenne du 4 juin 2021. Il est à noter que ces dernières doivent être adaptées selon que le transfert de données relève uniquement de la LPD (ou de la nLPD) ou qu'il dépend à la fois de la LPD et du RGPD (cf. www.swissprivacy.law/91).

Afin d'examiner les « garanties suffisantes » que l'exportateur doit offrir, le PFPDT exige au préalable une analyse portant sur l'accès des autorités du pays tiers aux données, ainsi que

les droits des personnes concernées. Le PFPDT exige ici une analyse très – à notre sens trop – poussée puisqu'il est précisé que celle-ci doit prendre en compte notamment (i) les prescriptions juridiques en vigueur dans le pays de destination, (ii) la pratique des autorités administratives et des autorités judiciaires et (iii) la jurisprudence. Compte tenu de la complexité de l'analyse qui s'apparente à une étude d'un ordre juridique étranger, celle-ci devra souvent être conduite au moyen d'un avis de droit indépendant.

Comme indiqué auparavant, cet examen vise à déterminer le risque que des autorités étrangères puissent avoir accès aux données transférées, respectivement à déterminer les droits des personnes concernées. Selon le PFPDT, cet examen doit permettre de mettre en lumière les lacunes du droit étranger en le comparant aux garanties fondamentales reconnues en Suisse, soit :

- Légalité : base légale suffisamment claire et précise concernant les buts, la procédure d'accès aux données par les autorités, les conditions juridiques matérielles de cet accès et les prérogatives des autorités en question ;
- Proportionnalité : les prérogatives des autorités et les mesures qu'elles prennent doivent être appropriées et nécessaires pour atteindre les buts légaux de l'accès des autorités aux données. Elles doivent également être raisonnablement exigibles ;
- Voies de droits effectives : en Suisse, les personnes concernées doivent disposer de voies de droit effectives, inscrites dans la loi, pour faire valoir leurs droits en matière de protection de la sphère privée et d'autodétermination informationnelle ; et
- Garantie de l'accès au juge et à un tribunal indépendant et impartial : les atteintes à la vie privée et l'autodétermination informationnelle doivent être soumises à un système de contrôle efficace, indépendant et impartial.

III. Examen de la nécessité de mettre en place des mesures de protection

Lorsque l'analyse décrite ci-dessus est terminée, elle peut démontrer (i) soit que les garanties sont assurées (ii) soit que les garanties ne sont pas assurées. Si l'analyse révèle que les garanties sont assurées, aucune mesure de protection additionnelle n'est nécessaire. Dans ce cas, si l'exportateur utilise les nouvelles clauses contractuelles types adoptées par la Commission européenne, aucune adaptation contractuelle n'est nécessaire.

Si au contraire, l'analyse révèle que les garanties ne sont pas assurées, des mesures de protection additionnelles doivent être prises. À ce sujet, il est important de relever que des mesures de protections de nature contractuelles ne sont pas suffisantes. En effet, comme le relève le PFPDT : « les mesures de nature contractuelles ne peuvent pas lier les autorités de

pays tiers et ne peuvent donc pas empêcher l'accès des autorités aux données ».

Au contraire, ces mesures de protection additionnelles doivent être de nature technique et organisationnelle. L'idée est en effet de mettre en place des mesures destinées à empêcher que les autorités du pays de destination ne puissent, dans les faits, accéder aux données personnelles transférées. Comme mesures de protection additionnelles, le PFPDT mentionne par exemple le chiffrement qui serait mis en œuvre selon le principe *Bring Your Own Key*, doublé du principe *Bring Your Own Encryption*, tout en admettant que ce type de mesures de protection n'est pas adapté en toutes circonstances.

Si l'examen démontre qu'il n'est pas possible de compenser les lacunes constatées dans le respect des garanties, le transfert de données vers l'étranger doit être immédiatement suspendu ou interrompu.

IV. Examen régulier de la situation

Après avoir mis en œuvre les mesures de protection supplémentaire, le PFPDT exige que l'exportateur de données vérifie régulièrement que les exigences techniques et juridiques soient respectées. Si l'exportateur arrive à la conclusion que les mesures de protection supplémentaires ne permettent pas (ou plus) de compenser les lacunes constatées, le transfert de données vers l'étranger doit être immédiatement suspendu ou interrompu.

Proposition de citation : Jeremy Reichlin / Livio di Tria, Le transfert de données à l'étranger : état des lieux en Suisse, 18 décembre 2022 *in* www.swissprivacy.law/191