Le Règlement Général sur la Protection des Données

Les transferts internationaux de données personnelles

Version du 16.04.2020

Contenu

Introduction 3

1. Transferts au sein de l'Espace économique européen (Union européenne, Liechtenstein, Norvège et Islande) 3

2. Transferts vers un pays en dehors de l'Espace économique européen disposant d'un niveau de protection adéquat 4

2.1. Le « EU-U.S. Privacy Shield Framework » 5

3. Transferts vers un pays en dehors de l'Espace économique européen ne disposant pas d'un niveau de protection adéquat 6

3.1. Clauses contractuelles 6

3.1.1. Clauses types de protection des données 6

3.1.2. Clauses contractuelles « ad hoc » 7

3.2. Règles d'entreprise contraignantes (BCR) 7

3.3. Codes de conduite et mécanismes de certification 10

3.4. Garanties spécifiques pour les transferts entre autorités ou organismes publics 10

3.5. Dérogations pour des situations particulières 11

4. La coopération internationale en matière policière et judiciaire 12

Introduction

Un transfert, vers un pays situé en dehors de l'Espace économique européen (Union européenne, Liechtenstein, Norvège et Islande) ou vers une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que dans certaines conditions.

Ces conditions particulières s'ajoutent aux obligations applicables aux responsables de traitement. Un test en deux étapes doit donc être appliqué:

- d'abord, une base juridique doit s'appliquer au traitement des données proprement dit, avec toutes les dispositions pertinentes du règlement général sur la protection des données (respect notamment du principe de licéité, compatibilité de la communication avec le traitement d'origine, information des personnes concernées) ;
- ensuite, les dispositions applicables aux transferts internationaux de données doivent être le cas échéant respectées.

Pour en savoir plus :

- chapitre V du règlement général pour la protection des données

1. Transferts au sein de l'Espace économique européen (Union européenne, Liechtenstein, Norvège et Islande)

Les données à caractère personnel peuvent circuler librement depuis le Grand-Duché de Luxembourg au sein de l'Espace économique européen, tant que les principes généraux du RGPD sont respectés.

En effet, les États membres appliquent le même niveau de protection lors du traitement de données à caractère personnel. Un transfert au sein de l'Espace économique européen est par conséquent régi de la même manière qu'un transfert au Luxembourg et doit par conséquent respecter les principes généraux du RGPD (respect notamment du principe de licéité, compatibilité de la communication avec le traitement d'origine, information des personnes concernées).

Pour en savoir plus :

- les obligations des responsables de traitement dans l'Espace économique européen ;
- dossier thématique sur l'impact du Brexit en matière de transferts internationaux de données

2. Transferts vers un pays en dehors de l'Espace économique européen disposant d'un niveau de protection adéquat

Tout responsable de traitement qui souhaite exporter des données à caractère personnel hors de l'Espace économique européen doit d'abord se renseigner sur le niveau de protection adéquat du pays destinataire. En effet, lorsque le pays tiers est considéré comme offrant un niveau de protection adéquat, le transfert peut être effectué comme s'il s'agissait d'un transfert au sein de l'Espace économique européen.

Il faudra néanmoins toujours respecter les principes généraux du RGPD (respect notamment du principe de licéité, compatibilité de la communication avec le traitement d'origine, information des personnes concernées).

C'est à la Commission européenne qu'il revient de constater par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat.

La Commission européenne a reconnu le caractère adéquat du niveau de protection des pays suivants :
- l'Andorre;
- l'Argentine;
- le Canada *(pour les traitements soumis à la loi canadienne « Personal Information Protection and Electronic Documentation Act »)*;
- les îles Féroé;
- Guernesey;
- l'Israël;
- l'île de Man;
- Jersey;
- la Nouvelle-Zélande;
- la Suisse;
- l'Uruguay; et
- les Etats-Unis d'Amérique *(pour les sociétés certifiées par le « EU-U.S. Privacy Shield Framework »)*.

La procédure d'adoption d'une décision d'adéquation de la Commission européenne concernant le Japon a été lancée le 5 septembre 2018. Des discussions sont également en cours concernant une potentielle décision d'adéquation de la Corée du Sud.

Pour en savoir plus :

- liste des pays tiers ayant fait l'objet d'une décision d'adéquation de la Commission européenne

2.1. Le « EU-U.S. Privacy Shield Framework »

Le « EU-U.S. Privacy Shield Framework », ou sphère du bouclier de protection des données Union européenne – Etats-Unis, est un ensemble de principes de protection des données personnelles auxquelles les entreprises établies aux Etats-Unis d'Amérique sont libres d'adhérer.

Les entreprises établies dans l'Espace économique européen peuvent transférer les données personnelles qu'elles traitent à destination des sociétés américaines figurant sur la liste « EU-U.S. Privacy Shield Framework », de la même manière que s'opèrent les transferts vers les pays reconnus comme "adéquats" par la Commission européenne.

Les principes que ces sociétés américaines doivent respecter, négociés entre les autorités américaines et la Commission européenne en 2016, sont basés sur ceux de la directive européenne 95/46/CE sur la protection des données, et ont été réévalués en 2017 et 2018 sur base du règlement général sur la protection des données. Ils entendent par ailleurs répondre aux faiblesses des précédents accords dits « Safe Harbor », négociés en 2001 et invalidés par la Cour de justice de l'Union européenne en 2015.

Pour en savoir plus :

- liste des sociétés américaines ayant adhéré au « EU-U.S. Privacy Shield Framework »
- explications sur le « EU-US Privacy Shield Framework » sur le site de la Commission européenne
- site web dédié au "EU-U.S. Privacy Shield Framework" (U.S. Department of Commerce)
- EU-US Privacy Shield - F A Q for European Businesses (Article 29 Working Party - WP 245)
- EU-US Privacy Shield - F A Q for European Individuals (Article 29 Working Party - WP 246)

3. Transferts vers un pays en dehors de l'Espace économique européen ne disposant pas d'un niveau de protection adéquat

Si le pays qui n'est pas membre de l'Espace économique européen (Union européenne, Liechtenstein, Norvège et Islande) ou l'organisation internationale vers lequel les données sont transférées n'a pas été reconnu comme adéquat par la Commission européenne, il existe cependant différentes possibilités pour un transfert de données.

Dans ce cas, la CNPD recommande d'adopter, tout comme ses homologues européens, une approche par étapes fondée sur les meilleures pratiques et consistant à envisager de fournir des garanties adéquates. Les exportateurs de données devraient donc d'abord s'efforcer de trouver des possibilités de procéder au transfert à l'aide de **garanties appropriées** (clauses contractuelles, règles d'entreprise contraignantes (BCR), codes de conduite, mécanismes de certification, ou garanties spécifiques pour le transfert entre autorités ou organismes publics), et ne recourir aux **dérogations** qu'en l'absence de telles garanties.

3.1. Clauses contractuelles

Diverses possibilités s'offrent aux responsables de traitement ou sous-traitants qui souhaitent transférer des données personnelles vers un pays en dehors de l'Espace économique européen ne disposant pas d'un niveau de protection adéquat: parmi celles-ci, l'utilisation d'un des modèles de « contrats-type » de la Commission européenne ou l'utilisation de clauses contractuelles proposées par l'entreprise.

3.1.1. Clauses types de protection des données

Afin d'aider les responsables de traitement, la Commission européenne met à leur disposition des modèles de « contrats-type » qui sont automatiquement considérés comme offrant des garanties suffisantes au regard de la réglementation en vigueur sur la protection des données.

Voici les modèles de contrats qui sont disponibles :

- clauses pour le transfert depuis un responsable de traitement dans l'U.E./E.E.E. vers un responsable de traitement hors U.E./E.E.E. (« C-to-C », deuxième modèle, tel qu'annexé dans la décision 2004/915/CE de la Commission européenne);
- clauses pour le transfert depuis un responsable de traitement dans l'U.E./E.E.E. vers un responsable de traitement hors U.E./E.E.E. (« C-to-C », premier modèle , tel qu'annexé dans la décision 2001/497/CE de la Commission européenne);
- clauses pour le transfert depuis un responsable de traitement dans l'U.E./E.E.E. vers un sous-traitant hors U.E./E.E.E. (« C-to-P », modèle annexé dans la décision 2010/87/UE de la Commission européenne).

Depuis le 25 mai 2018, il n'est plus nécessaire de demander l'autorisation préalable de la CNPD. Toutefois, le responsable de traitement ou le sous-traitant doit toujours être en mesure de

transmettre ces clauses à la CNPD si elle le demande (par exemple, en cas de contrôle ou d'audit).

Pour en savoir plus :

- explications sur les clauses types de protection des données sur le site de la Commission européenne ;
- F.A.Q. adoptées par le groupe de travail « article 29 » (prédécesseur de l'EDPB) à propos des clauses « C-to-P » (WP176).

3.1.2. Clauses contractuelles « ad hoc »

Si le responsable de traitement n'opte pas pour un modèle de la Commission européenne, il peut néanmoins rédiger ses propres clauses contractuelles (clauses « ad hoc ») qui devront apporter des garanties suffisantes au regard de la protection des données. Ces clauses doivent conformément à l'article 46 paragraphe (3) lettre (a) du RGPD être autorisées par la CNPD, et soumises conformément à l'article 46 paragraphe (4) du RGPD au mécanisme de cohérence, c'est-à-dire que ces clauses devront être approuvées par l'EDPB.

Conformément au règlement N°7/2020 du 3 avril 2020 fixant le montant et les modalités de paiement des redevances dans le cadre de ses pouvoirs d'autorisation et de consultation de la CNPD, tout responsable du traitement ou sous-traitant, établi sur le territoire luxembourgeois, qui soumet pour autorisation des clauses contractuelles à la CNPD conformément à l'article 46, paragraphe 3, lettre a) du RGPD, doit verser une redevance d'un montant de 1.500 € à la CNPD.

Pour en savoir plus :

- modèle de clauses « ad hoc » pour le transfert depuis un sous-traitant dans l'U.E./E.E.A. vers un sous-traitant hors U.E./E.E.A. (« P-to-P »), adoptées par le groupe de travail « article 29 » (prédécesseur de l'EDPB) (WP214)

3.2. Règles d'entreprise contraignantes (BCR)

Les règles d'entreprise contraignantes (en anglais « binding corporate rules », ou BCR) permettent d'assurer un niveau de protection suffisant aux données transférées au sein d'un groupe d'entreprise tant à l'intérieur qu'à l'extérieur de l'Espace économique européen. Cette garantie appropriée se prête surtout aux groupes internationaux d'entreprises mettant en œuvre un grand nombre de transferts internationaux de données.

Les BCR désignent une « charte de la protection des données » personnelles élaborée par un groupe d'entreprises qui définit sa politique en matière de transferts de données à caractère personnel. Cette charte doit être contraignante et respectée par toutes les entités du groupe, quel que soit leur pays d'implantation, ainsi que par tous leurs employés. En outre, elle doit conférer aux personnes concernées (clients, fournisseurs et/ou employés) des droits opposables en ce qui concerne le traitement de leurs données à caractère personnel.

Les BCR présentent de nombreux avantages pour un groupe d'entreprises multinationales :

- conformité avec le règlement général sur la protection des données (article 47);
- limitation des garanties appropriées à mettre en œuvre pour chaque transfert (par exemple, l'adoption de BCR au niveau du groupe évite de devoir signer autant de clauses types de protection des données qu'il y a de transferts) ;
- uniformisation des pratiques relatives à la protection des données au sein d'un groupe ;
- guide interne en matière de protection des données personnelles, qui participe à la responsabilisation du groupe vis-à-vis du RGPD ;
- moyen plus flexible et adapté à la culture d'entreprise ;
- possibilité de placer la protection des données au rang de "préoccupation éthique du groupe".

Procédure d'approbation des BCR

La procédure d'approbation des BCR est prévue dans les dispositions du RGPD (articles 47, 63, 64 et 65), et plus amplement détaillée dans le document de travail WP263 rev.01 adopté le 11 avril 2018 par le groupe « article 29 » sur la protection des données, prédécesseur du comité européen de la protection des données (en anglais, European Data Protection Board ou « EDPB »).

Elle s'opère en plusieurs étapes :

- identification de l'autorité de supervision principale (« lead authority »),
- procédure de coopération européenne entre l'autorité de supervision principale (« lead authority »), les autorités secondaires (« co-reviewers ») et les autres autorités concernées,
- avis (non contraignant) de l'EDPB au sujet du projet de décision consolidé soumis par l'autorité de supervision compétente,
- approbation (ou non) des BCR par l'autorité de supervision principale, en tenant compte de l'avis de l'EDPB.

Conformément au règlement N°7/2020 du 3 avril 2020 fixant le montant et les modalités de paiement des redevances dans le cadre de ses pouvoirs d'autorisation et de consultation de la CNPD, tout groupe d'entreprise établi sur le territoire luxembourgeois, qui soumet pour approbation des règles d'entreprise contraignantes à la CNPD en application de l'article 47 du RGPD, doit verser une redevance d'un montant de 1.500 € à la CNPD.

Pour en savoir plus :

- Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR (WP263 rev.01)
- Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, (WP 264)
- Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data (WP 265)
- Working Document on Binding Corporate Rules for Controllers (WP256rev.01)
- Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (WP 257 rev.01)

- explication de la procédure d'approbation de BCR sur le site de la Commission européenne
- explication de la procédure d'approbation de BCR sur le site de l'autorité belge de protection des données

3.3. Codes de conduite et mécanismes de certification

Depuis l'entrée en application du RGPD le 25 mai 2018, de nouvelles possibilités s'offrent aux responsables de traitement ou sous-traitants qui souhaitent transférer des données personnelles vers un pays en dehors de l'Espace économique européen ne disposant pas d'un niveau de protection adéquat, outre les clauses contractuelles et les règles d'entreprise contraignantes. Il s'agit :

- de codes de conduite approuvés conformément à l'article 40 du RGPD, assortis de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées ; et

- de mécanismes de certification approuvés conformément à l'article 42 du RGPD, assortis de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

Pour en savoir plus :

- article 46 du règlement général pour la protection des données
- Comité européen de la protection des données, guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 - version for public consultation

3.4. Garanties spécifiques pour les transferts entre autorités ou organismes publics

Un transfert de données depuis une autorité ou un organisme public luxembourgeois, vers une autre autorité ou vers un autre organisme public situé dans un pays tiers (en-dehors de l'Espace économique européen) peut avoir lieu :

- par la signature d'un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics, sans que cela nécessite l'autorisation de la CNPD ;

- par des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées, qui doivent faire l'objet de l'autorisation de la CNPD, et soumises conformément à l'article 46 paragraphe (4) du RGPD au mécanisme de cohérence, c'est-à-dire que ces dispositions devront être approuvées par l'EDPB.

Pour en savoir plus :

- article 46 du règlement général pour la protection des données

3.5. Dérogations pour des situations particulières

Les dérogations visées à l'article 49 du règlement général sur la protection des données sont des exemptions au principe général selon lequel des données à caractère personnel ne peuvent être transférées vers des pays tiers que si un niveau de protection adéquat est offert dans le pays tiers ou si des garanties appropriées ont été apportées et si les personnes concernées bénéficient de droits opposables et effectifs afin de continuer à bénéficier de leurs droits fondamentaux et garanties.

Ces dérogations ne peuvent donc être utilisées que dans des situations particulières : les responsables de traitement doivent s'efforcer de mettre en place des garanties appropriées et ne doivent recourir à ces exceptions qu'en l'absence de telles garanties. L'article 49 du RGPD fait l'objet d'une interprétation stricte par les autorités de protection des données, afin que l'exception ne devienne pas la règle.

Parmi ces dérogations pour des situations particulières, on retrouve :

- le consentement explicite de la personne concernée au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées;
- la nécessité du transfert pour l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée;
- la nécessité du transfert pour la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale;
- la nécessité du transfert pour des motifs importants d'intérêt public;
- la nécessité du transfert pour la constatation, à l'exercice ou à la défense de droits en justice;
- la nécessité du transfert pour la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;
- le fait que le transfert ait lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit national, est destiné à fournir des informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit national ou le droit de l'État membre sont remplies dans le cas d'espèce.

Une dérogation de « dernier ressort » consiste à transférer des données à caractère personnel si c'est nécessaire aux fins des intérêts légitimes impérieux poursuivis par l'exportateur de données. Cependant, cette dérogation n'est applicable que si :

- aucune des dérogations pour des situations particulières visées ci-dessus n'est applicable,
- ce transfert ne revêt pas de caractère répétitif,
- ce transfert ne touche qu'un nombre limité de personnes concernées,
- ce transfert est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée,

- le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel,
- le responsable du traitement a informé l'autorité de contrôle (par exemple la CNPD) du transfert, et
- le responsable du traitement a informé la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit.

Pour en savoir plus :

- lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679, adoptées par l'EDPB le 25 mai 2018
- article 49 du règlement général pour la protection des données

4. La coopération internationale en matière policière et judiciaire

Des données à caractère personnel peuvent faire l'objet d'échanges entre autorités de différents pays dans le cadre de l'application de conventions ou règlements internationaux de coopération en matière policière ou judiciaire. Des autorités de contrôle communes veillent notamment à l'observation des principes de la protection des données dans le fonctionnement de Europol, Schengen, Eurodac et Eurojust.

Dans le cadre de la lutte contre le terrorisme et les associations criminelles, des accords ont été conclus entre l'Union européenne et certains de ses partenaires. Par exemple, les accords « Passenger Name Records » (PNR) imposent aux compagnies aériennes de communiquer à l'administration des douanes et aux services de sécurité américains des informations personnelles relatives aux passagers à destination des Etats-Unis d'Amérique. Des accords similaires ont été également signés avec le Canada et l'Australie. Par ailleurs, l'Union européenne a également signé un accord bilatéral avec les Etats-Unis concernant le transfert de données financières appelé « Terrorist Finance Tracking Programme » (TFTP).

Pour en savoir plus :

- explications sur les accords PNR et TFTP sur le site de la Commission européenne
- article 50 du règlement général sur la protection des données
- loi du 1er août 2018 relative au traitement des données des passagers aériens, chapitre 8