



Le règlement général sur la protection des données

Les transferts internationaux de données

3 avril 2025

Contenu

Introduction	3
Notion de transfert de données à caractère personnel vers un pays tiers	3
1. Transferts de données personnelles vers des pays en dehors de l'Espace économique européen avec un niveau de protection adéquat.....	6
2. Transferts de données à caractère personnel vers les États-Unis d'Amérique dans le cadre de protection des données UE-Etats-Unis.....	7
3. Transferts de données à caractère personnel vers des pays en dehors de l'Espace économique européen sans niveau de protection adéquat	9
3.1. Clauses contractuelles.....	11
3.1.1. Clauses contractuelles types adoptées par la Commission européenne	11
3.1.2. Clauses contractuelles « ad hoc »	12
3.2. Règles d'entreprise contraignantes (BCR)	13
3.3. Codes de conduite	15
3.4. Mécanismes de certification	16
3.5. Garanties spécifiques pour les transferts entre autorités ou organismes publics.....	18
4. Dérogations pour situations spécifiques.....	18

Introduction

Les règles de l'Union européenne en matière de protection des données s'appliquent dans l'Espace économique européen (à savoir l'Union européenne, le Liechtenstein, la Norvège et l'Islande, ci-après l'«EEE»). Les données à caractère personnel peuvent donc être transférées librement sur ce territoire, à condition que le traitement soit conforme aux [obligations générales applicables aux responsables du traitement et aux sous-traitants](#) prévues par le règlement général sur la protection des données 2016/679 (ci-après le « RGPD »).

Par contre, un transfert de données à caractère personnel qui font l'objet d'un traitement vers un pays situé en dehors de l'Espace économique européen (un « pays tiers ») ou vers une organisation internationale ne peut avoir lieu que dans certaines conditions décrites au chapitre V du RGPD. Ces conditions s'ajoutent aux obligations générales prévues par le RGPD. Par conséquent, une évaluation en deux étapes doit être appliquée:

- premièrement, le transfert de données à caractère personnel, en tant qu'activité de traitement, doit avoir une base de licéité et respecter toutes les dispositions pertinentes du RGPD (par exemple, les principes de licéité du traitement, de transparence, les conditions applicables aux situations de sous-traitance, etc.);
- deuxièmement, les dispositions applicables aux transferts internationaux de données prévues au chapitre V du RGPD doivent être respectées. Ainsi, les transferts de données à caractère personnel vers un pays tiers ne sont possibles que si :
 - o le transfert de données est couvert par une décision d'adéquation émise par la Commission européenne conformément à l'article 45 du RGPD
 - ou
 - o à défaut, si l'exportateur de données peut démontrer l'existence de garanties appropriées conformément à l'article 46 du RGPD
 - ou
 - o à défaut, si le transfert relève de l'une des dérogations prévues à l'article 49 du RGPD.

Notion de transfert de données à caractère personnel vers un pays tiers

Le RGPD ne définit pas les activités qui peuvent être qualifiées de transfert de données à caractère personnel vers un pays tiers. Afin de clarifier la notion de transfert de données à caractère personnel vers un pays tiers, le comité européen de la protection des données (ci-après le «CEPD») a publié les lignes directrices 5/2021 sur l'interaction entre l'application de l'article 3 et du chapitre V du RGPD¹, énonçant trois critères cumulatifs selon lesquels le traitement serait considéré comme un «transfert vers un pays tiers»:

¹ Comité européen de la protection des données (CEPD), lignes directrices 5/2021 du 18 novembre 2021 sur l'interaction entre l'application de l'article 3 et les dispositions relatives aux transferts internationaux conformément au chapitre V du RGPD.

1. le responsable du traitement ou le sous-traitant est soumis au RGPD pour le traitement donné,²
2. le responsable du traitement ou le sous-traitant (ci-après l'«exportateur de données») divulgue ou met d'une autre manière des données à caractère personnel à la disposition d'un *autre responsable du traitement*, d'un *autre responsable conjoint du traitement* ou d'un *autre* sous-traitant (ci-après l'«importateur de données») ³, et
3. l'importateur se trouve dans un pays tiers ou est une organisation internationale, que le RGPD soit ou non également applicable au traitement des données à caractère personnel mis en œuvre par l'importateur de données.⁴

Il convient de noter que les entités qui font partie du même groupe d'entreprises peuvent être considérées comme des responsables de traitement ou des sous-traitants distincts et que les divulgations de données entre ces entités pourraient être considérées comme des transferts de données à caractère personnel.⁵

Les exemples suivants constituent des «transferts» aux fins du RGPD:

- la société X établie au Luxembourg, agissant en tant que responsable du traitement, donne accès aux données personnelles de ses clients à une société Z établie au Chili, qui traite ces données en tant que sous-traitant pour le compte de X,⁶
- la société luxembourgeoise A, qui est une filiale de la société mère américaine B, communique les données à caractère personnel de ses employés à la société B afin qu'elles soient stockées dans une base de données RH centralisée par la société mère aux États-Unis. Dans ce cas, la société luxembourgeoise A traite (et divulgue) les données en sa qualité d'employeur et donc de responsable du traitement, tandis que la société mère est un sous-traitant. Dès lors, les données sont fournies par un responsable du traitement qui, en ce qui concerne le traitement en question, est soumis au RGPD, à un sous-traitant dans un pays tiers.

Les exemples suivants ne constituent pas des «transferts» aux fins du RGPD:

- les données à caractère personnel sont communiquées directement et de sa propre initiative par la personne concernée au destinataire. Dans ce cas, aucun responsable du traitement ou sous-traitant n'envoie ou ne met les données à disposition, c'est-à-dire qu'il n'y a pas d'«exportateur»,
- un salarié se rend dans un pays tiers et accède à distance aux données à caractère personnel traitées par l'employeur. L'accès à distance de données à caractère personnel à partir d'un pays tiers par le salarié ne constitue pas un transfert de données à caractère personnel, étant donné que le salarié fait partie intégrante du responsable du traitement,⁷

² Voir comité européen de la protection des données (CEPD), lignes directrices 3/2018 du 12 novembre 2019 sur le champ d'application territorial du RGPD (article 3).

³ Voir section 2.2 des lignes directrices 5/2021 susmentionnées.

⁴ Voir section 2.3 des lignes directrices 5/2021 susmentionnées.

⁵ Voir le point 16 des lignes directrices 5/2021 susmentionnées.

⁶ Voir le point 14 des lignes directrices 5/2021 susmentionnées.

⁷ *Idem*.

- un responsable du traitement ou un sous-traitant situé dans un pays tiers non soumis au RGPD transmet des données à caractère personnel à un responsable du traitement ou à un sous-traitant situé au Luxembourg.

Pour plus d'informations:

Article 3, chapitre V et considérants 101 à 116 du RGPD

Comité européen de la protection des données (CEPD), lignes directrices 3/2018 du 12 novembre 2019 sur le champ d'application territorial du RGPD (article 3), disponibles à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_fr

Comité européen de la protection des données (CEPD), lignes directrices 5/2021 sur l'interaction entre l'application de l'article 3 et les dispositions relatives aux transferts internationaux conformément au chapitre V du RGPD, version finale du 14 février 2023, disponible à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_fr

1. Transferts de données personnelles vers des pays en dehors de l'Espace économique européen avec un niveau de protection adéquat

Les responsables du traitement qui souhaitent transférer des données à caractère personnel en dehors de l'EEE doivent d'abord s'assurer que le pays de destination offre un niveau de protection adéquat.

Une «décision d'adéquation» est l'un des outils prévus par le RGPD permettant les transferts de données à caractère personnel de l'EEE vers des pays tiers (article 45 du RGPD). Plus précisément, la Commission européenne a le pouvoir d'adopter une décision d'adéquation établissant qu'un pays, un territoire, un ou plusieurs secteurs déterminés dans ce pays tiers, ou une organisation internationale offre un niveau adéquat de protection des données à caractère personnel. Lorsqu'une telle décision a été adoptée, le transfert peut être effectué de la même manière que s'il avait été effectué à l'intérieur de l'EEE.⁸ La Commission européenne a publié des décisions d'adéquation pour les pays suivants:

- [Andorre](#),
- [Argentine](#),
- [Canada](#) (pour les transferts aux destinataires assujettis à la loi canadienne sur la protection des renseignements personnels et les documents électroniques),
- [Îles Féroé](#),
- [Guernesey](#),
- [Israël](#),
- [Île de Man](#),
- [Japon](#),
- [Jersey](#),
- [Nouvelle-Zélande](#),
- [République de Corée](#),
- [Suisse](#) ,
- [Royaume-Uni](#)
- [États-Unis d'Amérique](#) (uniquement pour les entreprises certifiées au titre du cadre de protection des données UE-États-Unis: voir section suivante) et
- [Uruguay](#).

Les exportateurs de données devraient vérifier que leurs activités ou les catégories de données qu'ils traitent entrent dans le champ d'application de la décision d'adéquation qui constitue la base du transfert .

Pour plus d'informations:

- Article 45 et considérants 101 à 107 du RGPD Liste des pays tiers disposant d'une décision d'adéquation sur le site web de la Commission européenne, disponible à l'adresse suivante: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_fr
- Recommandations 1/2020 sur les mesures qui complètent les outils de transfert pour garantir le respect du niveau de protection des données à caractère personnel de l'UE:

⁸ Article 45 du RGPD.

2. Transferts de données à caractère personnel vers les États-Unis d'Amérique dans le cadre de protection des données UE-États-Unis

Le 10 juillet 2023, la Commission européenne a adopté une décision d'adéquation pour le cadre de protection des données UE-États-Unis (en anglais « EU-US Data Privacy Framework »), qui remplace le cadre du bouclier de protection des données (en anglais « Privacy Shield ») invalidé par la Cour de justice de l'Union européenne par la décision dite « Schrems II »⁹. À compter de cette date, les transferts de l'UE vers des entités et organisations aux États-Unis qui sont incluses dans la liste du « cadre de protection des données » peuvent être fondés sur la décision d'adéquation conformément à l'article 45 du RGPD et effectués librement, sans qu'il ne soit nécessaire de s'appuyer sur les outils de transfert de l'article 46 du RGPD (tels que décrits dans la section 3 de la présente guidance) ou d'appliquer des mesures supplémentaires pour encadrer les transferts vers les États-Unis.

Le cadre de protection des données UE-États-Unis introduit un système d'autocertification, qui oblige les entités américaines à respecter les obligations et les principes de protection des données énumérés dans ce cadre, tels que la limitation de la finalité et la minimisation des données, ainsi que le respect de certains droits des personnes concernées.

Ce mécanisme ainsi que l'application du cadre juridique aux États-Unis d'Amérique est suivi de manière permanente par la Commission européenne et les États membres de l'Union européenne. Si elle est en possession d'éléments indiquant qu'un niveau de protection adéquat n'est plus assuré, la Commission européenne peut décider de suspendre, de modifier ou d'abroger la décision d'adéquation, ou d'en restreindre le champ d'application.

Pour les entreprises basées au Luxembourg: dans quelles conditions les données peuvent-elles être transférées aux États-Unis?

Les entreprises, associations ou autres organisations établies au Luxembourg (ou dans un autre pays de l'EEE) qui transfèrent des données vers les États-Unis devraient consulter le site web du DPF, tenu à jour et mis à la disposition du public par le ministère américain du commerce (DoC), afin de vérifier si les entreprises auxquelles des données à caractère personnel seront transférées sont certifiées et respectent à ce titre les exigences-cadres. La liste des entités certifiées est disponible sur le site web du département américain du commerce <https://www.dataprivacyframework.gov/list>.

Il est important de noter que les transferts de données à caractère personnel à des entités aux États-Unis qui ne figurent pas sur la liste du cadre de protection des données UE-États-Unis ne peuvent pas se fonder sur la décision d'adéquation et doivent être effectués sur la base de l'un des outils de transfert prévus à l'article 46, paragraphe 2, du RGPD (voir section suivante).

⁹ Cour de Justice de l'Union européenne, 16 juillet 2020, Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems, affaire C-311/18.

Si l'entité américaine qui reçoit des données à caractère personnel aux États-Unis agit en tant que sous-traitant pour le compte de l'entité luxembourgeoise agissant en tant que responsable du traitement (par exemple, un fournisseur de services en nuage), un accord de traitement des données au titre de l'article 28 du RGPD sera requis, indépendamment de la participation de l'entreprise américaine (sous-traitant) au cadre de protection des données UE-États-Unis. De plus amples informations sur cette exigence peuvent être consultées dans la section «Contract Requirements for Data Transfers to a Processor» (Exigences contractuelles pour les transferts de données à un sous-traitant) de la FAQ – Cadre de protection des données UE-États-Unis (CPD UE-États-Unis) publiée sur le site web officiel du cadre de protection des données des États-Unis.¹⁰

Pour les personnes concernées établies au Luxembourg : Comment les personnes concernées peuvent-elles exercer leurs droits à l'égard d'une entreprise américaine certifiée ou déposer une plainte contre elle?

Vous trouverez de plus amples informations sur la manière dont les personnes concernées peuvent exercer leurs droits ou déposer une plainte dans le cadre du CPD sur notre page dédiée [\[lien\]](#).

Pour plus d'informations:

- Décision d'adéquation pour le cadre de protection des données UE-États-Unis [décision d'exécution de la Commission du 10 juillet 2023 conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil concernant le niveau adéquat de protection des données à caractère personnel au titre du cadre de protection des données UE-États-Unis]: https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_fr
- EDPB F.A.Q. on EU-U.S. Data Privacy Framework for European Businesses: https://www.edpb.europa.eu/system/files/2024-07/edpb_dpf_faq-for-businesses_en.pdf [\[en anglais\]](#)
- EDPB F.A.Q. on EU-U.S. Data Privacy Framework for European Individuals : https://www.edpb.europa.eu/system/files/2024-07/edpb_dpf_faq-for-individuals_en_0.pdf [\[en anglais\]](#)
- FAQ publiée sur le site web officiel du Cadre de protection des données des États-Unis: [https://www.dataprivacyframework.gov/program-articles/FAQs%E2%80%93EU%E2%80%93U.S.-Data-Privacy-Framework-\(EU%E2%80%93DPF\)](https://www.dataprivacyframework.gov/program-articles/FAQs%E2%80%93EU%E2%80%93U.S.-Data-Privacy-Framework-(EU%E2%80%93DPF)) [\[en anglais\]](#)

¹⁰ <https://www.dataprivacyframework.gov/program-articles/Contract-Requirements-for-Data-Transfers-to-a-Processor>

3. Transferts de données à caractère personnel vers des pays en dehors de l'Espace économique européen sans niveau de protection adéquat

En l'absence de décision d'adéquation (c'est-à-dire lorsqu'un pays, un territoire, un ou plusieurs secteurs spécifiques au sein de ce pays tiers ou une organisation internationale en dehors de l'EEE n'est pas reconnu par la Commission européenne comme offrant un niveau de protection adéquat), des transferts vers un pays tiers peuvent avoir lieu si l'exportateur de données a mis en place des «garanties appropriées».

L'article 46 du RGPD prévoit les garanties appropriées (ou «outils de transfert») suivantes:

- les clauses contractuelles types,
- des règles d'entreprise contraignantes,
- les codes de conduite,
- les mécanismes de certification et
- des garanties spécifiques pour les transferts entre autorités ou organismes publics.

Ce n'est qu'en l'absence de telles garanties appropriées que les exportateurs de données pourraient faire usage des dérogations prévues à l'article 49 du RGPD.¹¹

Conformément au principe de responsabilité¹², le responsable du traitement doit être en mesure de présenter, à la demande de la CNPD (par exemple, en cas de contrôle ou d'audit), l'une des garanties appropriées énumérées ci-dessus sur laquelle il s'appuie pour le transfert de données vers un pays situé en dehors de l'EEE ou vers une organisation internationale.

Dans ce contexte, il est important de mentionner que la Cour de justice de l'Union européenne (CJUE) a précisé dans son arrêt dit « Schrems II »¹³ qu'il ne suffit pas de démontrer la mise en œuvre des garanties appropriées énumérées à l'article 46 du RGPD. Les exportateurs de données (responsables du traitement et sous-traitants) qui s'appuient sur des garanties appropriées pour effectuer des transferts de données à caractère personnel vers des pays tiers doivent évaluer si des mesures supplémentaires à celles requises par les garanties appropriées sont nécessaires pour assurer une protection effective des données dans le cas d'espèce.

L'exportateur de données doit donc vérifier, avant tout transfert, au cas par cas, si l'outil de transfert sélectionné ou la garantie appropriée est efficace pour garantir que le niveau de protection accordé par le RGPD n'est pas compromis par le transfert en question. En particulier, l'exportateur de données doit évaluer si la législation et/ou la pratique du pays tiers vers lequel les données sont transférées peuvent affecter dans la pratique l'efficacité de l'outil de transfert sélectionné dans son cas spécifique, c'est-à-dire si cela empêche l'importateur de données de se conformer aux obligations qui lui incombent en vertu de l'outil de transfert. Si cette analyse d'impact du transfert révèle que l'outil de transfert sélectionné ne garantit pas, dans la pratique, que la personne concernée bénéficie d'un niveau de protection essentiellement équivalent à celui garanti au sein de l'Union européenne, l'exportateur de données doit vérifier, le cas échéant avec l'aide de l'importateur de données, s'il existe des mesures supplémentaires (de nature technique, organisationnelle ou contractuelle) qui pourraient permettre à l'outil de transfert d'être efficace

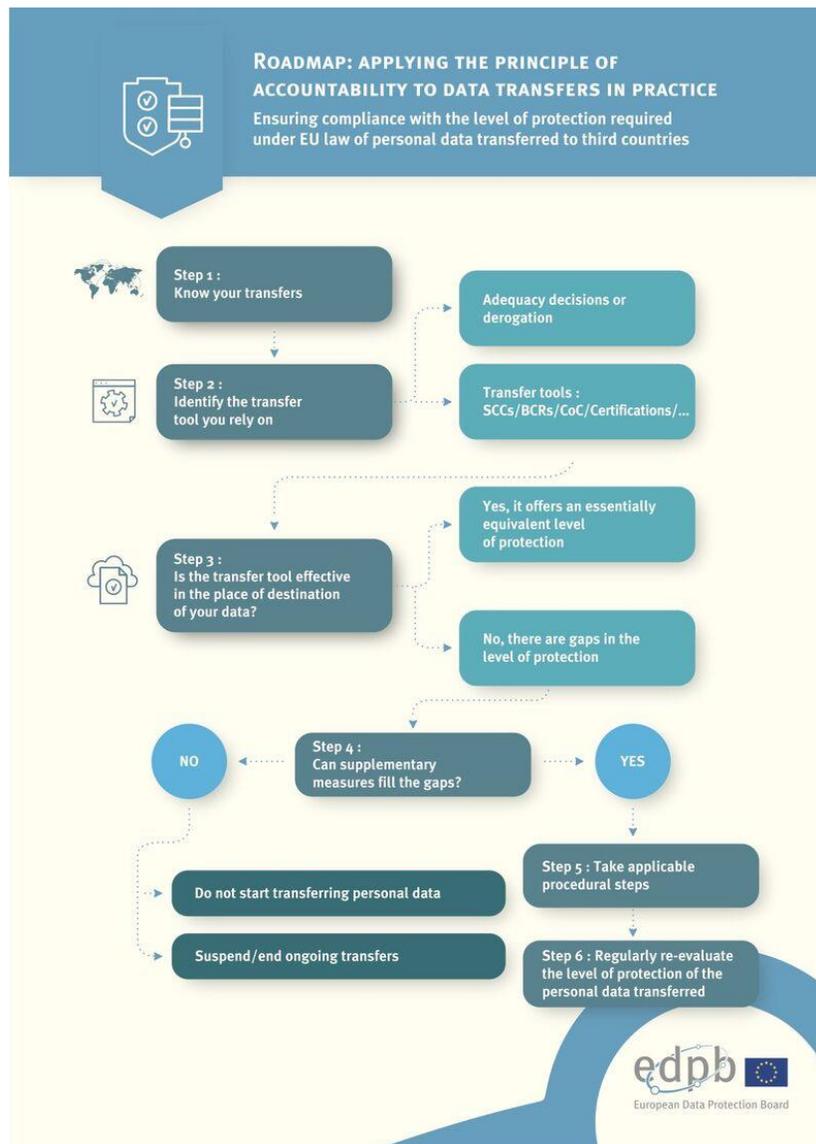
¹¹ Voir section 3.5 ci-dessous.

¹² Article 5, paragraphe 2, du RGPD.

¹³ Cour de Justice de l'Union européenne, 16 juillet 2020, Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems, affaire C-311/18.

pour assurer un niveau de protection essentiellement équivalent aux données transférées vers des pays tiers. Si de telles mesures supplémentaires existent, elles doivent être mises en œuvre ou, à défaut, le transfert doit être suspendu et/ou interrompu.

Le CEPD a adopté ses recommandations 01/2020 sur les mesures qui complètent les outils de transfert visant à garantir le respect du niveau de protection des données à caractère personnel de l'UE¹⁴ afin d'aider les responsables du traitement et les sous-traitants agissant en tant qu'exportateurs de données à s'acquitter de leur devoir d'identifier et de mettre en œuvre des mesures supplémentaires appropriées. Ces recommandations contiennent une approche en six étapes de l'analyse d'impact des transferts, qui sont illustrées dans la feuille de route suivante pour l'évaluation de la conformité des transferts avec les dispositions de l'article chapitre V du RGPD.



¹⁴ Comité européen de la protection des données, recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, 18 juin 2021 (version 2.0).

Pour plus d'informations:

- Comité européen de la protection des données, recommandations 1/2020 du 18 juin 2021 sur les mesures qui complètent les outils de transfert pour garantir le respect du niveau de protection des données à caractère personnel de l'UE, disponibles à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_fr
- Comité européen de la protection des données, Foire aux questions (FAQ) du 24 juillet 2020 sur l'arrêt de la Cour de justice de l'Union européenne dans l'affaire C-311/18, Data Protection Commissioner/Facebook Ireland Ltd et Maximilian Schrems, disponible à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_fr
- [Guide pratique sur l'évaluation de l'impact des transferts de l'autorité française de protection des données \(CNIL\)](#)

3.1. Clauses contractuelles

Comme indiqué au point 3, les responsables du traitement et les sous-traitants doivent se baser sur l'une des garanties appropriées pour transférer des données à caractère personnel vers des pays extérieurs à l'EEE qui n'offrent pas un niveau de protection adéquat. L'une des garanties prévues par le RGPD est l'utilisation de clauses contractuelles adoptées par la Commission européenne (article 46, paragraphe 2, lettre c) du RGPD) ou adoptées par une autorité de contrôle nationale et approuvées par la Commission européenne (article 46, paragraphe 2, lettre d) du RGPD). Une autre garantie appropriée est l'utilisation de clauses contractuelles dites « ad hoc », rédigées par les exportateurs de données et autorisées par une autorité de contrôle nationale, qui contiennent des garanties suffisantes pour protéger les transferts de données personnelles (article 46, paragraphe 3, lettre a) du RGPD). Tant les clauses contractuelles « types » que les clauses contractuelles « ad hoc » constituent des contrats liants ceux qui envoient les données (exportateurs de données) et ceux qui les reçoivent (importateurs de données).

3.1.1. Clauses contractuelles types adoptées par la Commission européenne

Les responsables de traitement et les sous-traitants soumis au RGPD, y compris ceux établis en dehors de l'EEE, ¹⁵ peuvent se fonder sur les clauses contractuelles types (« CCT », en anglais « standard contractual clauses » ou « SCC ») émises par la Commission européenne.^{16 17}

Les CCT suivent une approche modulaire pour permettre de répondre à plusieurs scénarios de transfert. Ils contiennent quatre ensembles de clauses (modules) en fonction du rôle de

¹⁵ Sous réserve du RGPD en vertu de l'article 3 du RGPD.

¹⁶ Décision d'exécution (UE) 2021/914 de la Commission européenne du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil.

¹⁷ Les CCT ont été mises à jour le 4 juin 2021 et remplacent les CCT précédemment applicables.

l'exportateur et de l'importateur de données en tant que sous-traitant ou responsable du traitement:

- Module 1: transfert d'un responsable du traitement à un responsable du traitement («C2C»),
- Module 2: transfert d'un responsable du traitement à un sous-traitant («C2P»),
- Module 3: transfert d'un sous-traitant à un sous-traitant («P2P»),
- Module 4: transfert d'un sous-traitant à un responsable du traitement («P2C»).

Les CCT doivent être signées avec qu'un transfert n'ait lieu. Il convient de noter que les CCT contiennent une clause d'amarrage qui permet à d'autres exportateurs ou importateurs de données d'adhérer aux CCT tout au long du cycle de vie du contrat (article 7 des CCT).

Les CCT aident les exportateurs et les importateurs de données à se conformer à l'exigence d'une analyse d'impact du transfert et à mettre en œuvre des mesures supplémentaires, comme indiqué dans l'arrêt Schrems II.

Ainsi, la section III («législations et obligations locales en cas d'accès par les autorités publiques») des CCT énonce ce qui suit:

- l'exportateur de données (avec l'aide de l'importateur de données) est tenu de tenir compte du niveau de protection dans le pays tiers en question, des circonstances spécifiques du transfert et de toute mesure technique et organisationnelle à mettre en place pour compléter les CCT, et
- l'importateur de données a l'obligation de notifier à l'exportateur de données tout changement dans la situation dans le pays tiers qui crée une incapacité à se conformer aux CCT. Dans ce cas, l'exportateur doit adopter des mesures appropriées pour remédier à la situation ou suspendre le transfert.

En outre, les CCT contiennent des exemples pratiques de mesures techniques supplémentaires, telles que le cryptage.

3.1.2. Clauses contractuelles « ad hoc »

Les exportateurs de données peuvent également s'appuyer sur des «clauses ad hoc»,¹⁸ qui peuvent par exemple traiter de la situation dans laquelle des données à caractère personnel sont initialement transférées par un responsable du traitement à un sous-traitant au sein de l'UE, puis transférées par le sous-traitant (exportateur de données) à un sous-traitant dans un pays tiers (importateur de données) et à des sous-traitants ultérieurs. Les exportateurs de données souhaitant utiliser des clauses ad hoc doivent obtenir une autorisation de l'autorité de contrôle compétente (par exemple, la CNPD) qui va se coordonner avec les autres autorités de contrôle conformément au mécanisme mis en place par l'article 63 du RGPD.¹⁹

Conformément au règlement no 7/2020 de la CNPD 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, chaque responsable du traitement ou sous-traitant établi sur le territoire

¹⁸ Article 46, paragraphe 3, point a), du RGPD.

¹⁹ Article 46, paragraphe 4, du RGPD.

luxembourgeois, qui soumet des clauses contractuelles d'autorisation à la CNPD conformément à l'article 46, paragraphe 3, point a), du RGPD, doit payer une redevance de 1 500 EUR à la CNPD²⁰.

Plus d'informations:

- Article 46 et considérants 108, 109 et 114 du RGPD
- Clauses contractuelles types adoptées par la Commission européenne (décision d'exécution (UE) 2021/914 de la Commission européenne du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil): https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
- Groupe de travail «Article 29», document de travail 01/2014 du 21 mars 2014 sur le projet de clauses contractuelles «ad hoc» «sous-traitant de l'UE vers un sous-traitant ultérieur non UE» («P-to-P») (WP214), disponible à l'adresse suivante: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp214_fr.pdf [en anglais]

3.2. Règles d'entreprise contraignantes (BCR)

En l'absence de décision d'adéquation, les exportateurs de données peuvent se fonder sur des règles d'entreprise contraignantes (en anglais « binding corporate rules » ou « BCR »), qui sont conçues pour permettre aux groupes d'entreprises et aux organisations multinationales de transférer des données à caractère personnel de l'EEE vers des entités affiliées situées en dehors de l'EEE, conformément au chapitre V du RGPD.²¹

Les BCR sont des règles internes adoptées par un groupe d'entreprises, qui définissent sa politique globale en matière de transferts internationaux de données à caractère personnel. Ces règles doivent être contraignantes et respectées par toutes les entités du groupe, quel que soit leur pays d'établissement, ainsi que par tous leurs employés. En outre, elles doivent expressément conférer des droits opposables aux personnes concernées en ce qui concerne le traitement de leurs données à caractère personnel.

Il existe deux types différents de BCR. Le choix du type correct de BCR est important étant donné qu'elles couvrent des situations différentes qui sont sujettes à des exigences différentes en ce qui concerne le contenu des BCR, comme précisé à l'article 47 du RGPD.

Les BCR pour responsables de traitement (dites « BCR-C ») couvrent les transferts d'une entité du groupe établie dans l'EEE et agissant en tant que responsable du traitement vers une autre entité du groupe établie dans le pays tiers qui agit en tant que sous-traitant ou sous-traitant ultérieur. De plus amples informations sur le champ d'application et les exigences des BCR-C

²⁰ Disponible sous : <https://cnpd.public.lu/content/dam/cnpd/fr/decisions-avis/2020/07-2020-reglement-CNPD-redevances-signé.pdf>.

²¹ Article 46, paragraphe 2, et article 47 du RGPD.

sont disponibles dans le référentiel du CEPD pour les responsables du traitement, adopté le 20 juin 2023.²²

Les BCR pour sous-traitants (dites « BCR-P ») couvrent les transferts d'une entité du groupe établie dans l'EEE et agissant en tant que sous-traitant pour un responsable du traitement externe vers une autre entité du groupe en tant que sous-traitant. De plus amples informations sur le champ d'application et les exigences des BCR-P sont disponibles dans le document de travail modifié du groupe de travail « article 29 » (WP29) sur les règles d'entreprise contraignantes pour les transformateurs (wp257rev).²³

Les BCR sont approuvées par l'autorité de contrôle compétente, qui se coordonnent avec les autres autorités de contrôle, conformément au mécanisme de contrôle de la cohérence prévu à l'article 63 du RGPD.

Processus d'approbation des BCR

La procédure d'approbation des règles d'entreprise contraignantes pour les responsables du traitement et pour les sous-traitants est définie à l'article 47, paragraphe 1, et aux articles 63 à 65 du RGPD.

Le processus d'approbation des BCR comprend les étapes suivantes:²⁴

1. identification de l'autorité de contrôle chef de file pour l'approbation des BCR,
2. procédure de coopération pour l'approbation des BCR entre l'autorité de contrôle chef de file, les autorités de contrôle agissant en tant qu'autorités secondaires et les autres autorités de contrôle concernées,
3. adoption de l'avis du comité européen de la protection des données,²⁵
4. adoption d'une décision nationale par l'autorité de contrôle chef de file, en tenant compte de l'avis du comité européen de la protection des données.

Conformément à l'article 6 du règlement no 7/2020 de la CNPD du 3 avril 2020²⁶ fixant le montant et les modalités de paiement des redevances dans le cadre de ses pouvoirs d'autorisation et de consultation, chaque groupe d'entreprises établi sur le territoire luxembourgeois, qui soumet des règles d'entreprise contraignantes à la CNPD pour approbation conformément à l'article 47 du RGPD, doit payer une redevance de 1 500 EUR à la CNPD.

²² Recommandations 1/2022 de l'EDPB sur la demande d'approbation et sur les éléments et principes figurant dans les règles d'entreprise contraignantes du contrôleur disponibles à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-12022-application-approval-and_fr

Document 23 de travail sur les règles d'entreprise contraignantes pour les sous-traitants (wp257rev.01): <https://ec.europa.eu/newsroom/article29/items/614110>

²⁴ Article 47, paragraphe 1, article 63 et article 64, paragraphe 1, point f), du RGPD et document de travail du groupe de travail « Article 29 » du 11 avril 2018 établissant une procédure de coopération pour l'approbation de « règles d'entreprise contraignantes » pour les responsables du traitement et les sous-traitants au titre du RGPD (WP263rev.01), approuvé par le comité européen de la protection des données le 25 mai 2018.

²⁵ Conformément à l'article 64, paragraphe 3, du RGPD.

²⁶ Disponible sous : <https://cnpd.public.lu/content/dam/cnpd/fr/decisions-avis/2020/07-2020-reglement-CNPD-redevances-signé.pdf>.

Pour plus d'informations:

- Informations sur les règles d'entreprise contraignantes sur le site web de la Commission européenne, disponibles à l'adresse suivante: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_fr [en anglais]
- Lignes directrices 8/2022 du comité européen de la protection des données sur l'identification de l'autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant, disponibles à l'adresse suivante: https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202208_identifying_isa_targeted_update_v2_fr.pdf
- Recommandations 1/2022 du comité européen de la protection des données concernant la demande d'approbation et les éléments et principes des règles d'entreprise contraignantes pour les responsables du traitement (dit « référentiel BCR-C »): https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-12022-application-approval-and_fr
- Document de travail sur les règles d'entreprise contraignantes pour les sous-traitants (wp257rev.01): <https://ec.europa.eu/newsroom/article29/items/614110>
- Recommandation concernant le formulaire type de demande d'approbation du formulaire «Règles d'entreprise contraignantes pour les sous-traitants» (wp265): <https://ec.europa.eu/newsroom/article29/items/623848/fr>

3.3. Codes de conduite

En l'absence de décision d'adéquation, les exportateurs de données (responsables de traitement et sous-traitants) peuvent s'appuyer sur des codes de conduite approuvés²⁷ en tant que garanties appropriées pour les transferts de données à caractère personnel vers des pays tiers.

Les codes de conduite sont généralement rédigés par des entités, des associations ou des fédérations qui représentent de grandes catégories de responsables du traitement et de sous-traitants, telles que des associations sectorielles.

Les codes de conduite doivent être approuvés par l'autorité de contrôle compétente et respecter les exigences spécifiques énoncées à l'article 40 et à l'article 46, paragraphe 2, point e), du RGPD et aux lignes directrices 04/2021 du comité européen de la protection des données sur les codes de conduite en tant qu'outils de transfert afin de constituer des garanties appropriées dans le cadre des transferts de données à caractère personnel vers des pays tiers ou des organisations internationales.

Une fois approuvé par l'autorité de contrôle compétente, les exportateurs de données peuvent adhérer à un code de conduite.²⁸ De plus, ces exportateurs doivent fournir des engagements contraignants et exécutoires destinés à confirmer que le code de conduite en question assure effectivement des garanties appropriées pour les transferts de données en dehors de l'EEE

De plus amples informations sont disponibles dans les lignes directrices 01/2019 du comité européen de la protection des données sur les codes de conduite et les organismes de contrôle,

²⁷ Article 46, paragraphe 2, point e), du RGPD.

²⁸ Article 40, paragraphes 3 et 9, et article 46, paragraphe 2, point e), du RGPD.

ainsi que dans les lignes directrices 04/2021 du comité européen de la protection des données sur les codes de conduite en tant qu'outils pour les transferts.

Pour plus d'informations:

- Articles 40, 41 et 46 et considérants 98, 99 et 114 du RGPD.
- Lignes directrices 1/2019 sur les codes de conduite et les organismes de suivi au titre du règlement (UE) 2016/679, adoptées le 4 juin 2019: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_fr
- Comité européen de la protection des données, lignes directrices 04/2021 du 22 février 2022 sur les codes de conduite en tant qu'outils pour les transferts, disponibles à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_fr

3.4. Mécanismes de certification

En l'absence de décision d'adéquation, les exportateurs de données (responsables de traitement et sous-traitants) peuvent s'appuyer sur des mécanismes de certification en tant que garanties appropriées pour les transferts de données à caractère personnel vers des pays tiers.²⁹ Des mécanismes de certification peuvent être élaborés et mis en place pour démontrer l'existence de garanties appropriées fournies par les importateurs de données (responsables du traitement ou sous-traitants) dans le pays tiers afin de permettre les transferts de données à caractère personnel vers des pays tiers.³⁰ Les importateurs de données (responsables du traitement ou sous-traitants) certifiés dans des pays tiers doivent, en plus de la certification, prendre des engagements contraignants et exécutoires d'appliquer les garanties sur lesquelles la certification est fondée.³¹

Les mécanismes de certification doivent être approuvés par l'autorité de contrôle compétente et se conformer à l'article 42 et à l'article 46, paragraphe 2, point f), du RGPD,³² ainsi qu'aux lignes directrices 07/2022 de l'EDPB sur la certification en tant qu'outil de transfert³³, afin de constituer des garanties appropriées dans le cadre des transferts de données à caractère personnel vers des pays tiers ou des organisations internationales. De plus amples informations sont disponibles dans les lignes directrices 07/2022 du comité européen de la protection des données sur la certification en tant qu'outil de transfert. Ces lignes directrices fournissent des orientations sur des aspects spécifiques concernant la certification en tant qu'outil de transfert, tels que l'objectif, le champ d'application et les différents acteurs concernés. En outre, ils contiennent des exigences spécifiques pour l'accréditation d'un organisme de certification et des critères de certification spécifiques visant à démontrer l'existence de garanties appropriées pour les transferts. Enfin, ils précisent les éléments qui devraient être abordés dans les engagements contraignants et

²⁹ Article 46, paragraphe 2, point f), du RGPD.

³⁰ Articles 42 et 46, paragraphe 2, point f), du RGPD.

³¹ Article 42, paragraphe 2, du RGPD.

³² Voir les articles 40, 42 et 46 du RGPD.

³³ Comité européen de la protection des données, lignes directrices 07/2022 sur la certification en tant qu'outil de transfert, 14 février 2023.

exécutoires que les importateurs de données (responsables du traitement ou sous-traitants) dans le pays tiers non soumis au RGPD devraient prendre aux fins de fournir des garanties appropriées aux données transférées vers des pays tiers.

La certification en tant que transfert d'outil peut couvrir les transferts de tous les pays de l'UE (« UE-Seal ») ou simplement les transferts d'un État membre de l'UE vers les pays tiers (certification nationale). Dans ce dernier cas, l'autorité nationale approuve le mécanisme de certification à la suite d'un avis du comité européen de la protection des données. Dans le cas d'un « EU-Seal », l'EDPB approuve le mécanisme de certification. Une fois que la certification en tant qu'outil de transfert est approuvée, les importateurs de données de pays tiers peuvent demander la certification par des organismes de certification. Les exportateurs de données qui transfèrent des données à des importateurs de données certifiés peuvent alors se baser sur le mécanisme de certification comme garantie appropriée.

De plus amples informations sur la procédure d'approbation figurent dans les lignes directrices 1/2018 du comité européen de la protection des données relatives à la certification et à l'identification des critères de certification conformément aux articles 42 et 43 du règlement.

Conformément à l'article 4 du règlement no 7/2020 de la Commission nationale de la protection des données 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, chaque « scheme owner », qui soumet à la CNPD une demande d'approbation d'un mécanisme certification conformément à l'article 42, paragraphe 5, du RGPD, doit payer à la CNPD une redevance dont le montant dépend de l'étape de la procédure.

Pour plus d'informations:

- Articles 42, 43 et 46 et considérants 100 et 114 du RGPD.
- Comité européen de la protection des données, lignes directrices 1/2018 du 4 juin 2019 sur la certification et l'identification des critères de certification conformément aux articles 42 et 43 du règlement 2016/679, disponibles à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_fr
- Comité européen de la protection des données, lignes directrices 4/2018 du 4 juin 2019 sur l'accréditation des organismes de certification au titre de l'article 43 du règlement général sur la protection des données (2016/679), disponibles à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_fr
- Lignes directrices 07/2022 sur la certification en tant qu'outil de transfert, adoptées le 14 février 2023: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_fr

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

Les transferts d'une autorité ou d'un organisme public de l'EEE vers une autre autorité ou un autre organisme public d'un pays tiers peuvent avoir lieu:

- sur base d'un acte juridiquement contraignant et exécutoire entre autorités ou organismes publics, sans qu'une autorisation préalable de la CNPD³⁴ ne soit requise, ou
- si une autorité ou un organisme public n'a pas le pouvoir de conclure des arrangements juridiquement contraignants et exécutoires, au moyen d'arrangements administratifs, qui peuvent être conclus entre des autorités ou organismes publics et qui prévoient des droits opposables et effectifs des personnes concernées et des voies de recours effectives, à condition d'obtenir au préalable l'autorisation préalable de la CNPD conformément au mécanisme de contrôle de la cohérence prévu à l'article 63 du RGPD.³⁵

Pour plus d'informations:

- Comité européen de la protection des données, avis 4/2019 du 12 février 2019 sur le projet d'accord d'association entre les autorités de surveillance financière de l'EEE et de pays tiers, disponible à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-42019-draft-aa-between-eea-and-non-eea_fr
- Comité européen de la protection des données, lignes directrices 2/2020 du 15 décembre 2020 sur l'article 46, paragraphe 2, point a), et l'article 46, paragraphe 3, point b), du règlement (UE) 2016/679 pour les transferts de données à caractère personnel entre autorités et organismes publics de l'EEE et de pays tiers, disponibles à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_fr
- Comité européen de la protection des données, Toolbox of 14 March 2022 on essential data protection safeguards for enforcement cooperation between EEA data protection authorities and competent data protection authorities of third countries, disponible à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/toolbox-essential-data-protection-safeguards-enforcement-cooperation_fr

4. Dérogations pour situations spécifiques

L'article 49 du RGPD énumère de manière exhaustive un certain nombre de dérogations. Il s'agit de dérogations au principe général selon lequel les données à caractère personnel ne peuvent être transférées vers des pays tiers que si un niveau de protection adéquat est prévu dans le pays tiers ou si des garanties appropriées ont été apportées, tel que décrit dans les sections précédentes.

Ces dérogations ne doivent donc être utilisées que dans les situations spécifiques énumérées ci-dessous. Ce n'est que s'il n'est pas possible de se fonder sur une décision d'adéquation ou une des garanties appropriées visées à l'article 46 du RGPD, que les responsables du traitement ou

³⁴ Article 46, paragraphe 2, point a), du RGPD.

³⁵ Article 46, paragraphes 3, point b), et 4, du RGPD.

les sous-traitants pourraient faire usage de l'une des dérogations prévues par l'article 49 du RGPD. Lorsqu'ils s'appuient sur ces dérogations, les responsables du traitement devraient être en mesure de démontrer pourquoi il n'a pas été possible de s'appuyer sur des garanties appropriées, comme l'exige le principe de «responsabilité».

Sur la base des dérogations, les données à caractère personnel peuvent être transférées vers un pays tiers lorsque:

- la personne concernée a explicitement consenti au transfert proposé, après avoir été informée des risques éventuels de tels transferts pour la personne concernée en raison de l'absence de décision d'adéquation et de garanties appropriées;
- le transfert est nécessaire à 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;
- le transfert est nécessaire à 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;
- le transfert est nécessaire pour des raisons importantes d'intérêt public;
- le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice;
- le transfert est nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée est physiquement ou juridiquement incapable de donner son consentement; ou
- le transfert est effectué à partir d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à informer le public et qui est ouvert à la consultation du public en général ou de toute personne pouvant démontrer un intérêt légitime, mais uniquement dans la mesure où les conditions prévues par le droit de l'Union ou le droit d'un État membre pour la consultation sont remplies dans le cas d'espèce.

En tant que dérogation de « dernier recours », les données à caractère personnel peuvent être transférées si cela est nécessaire aux fins des intérêts légitimes impérieux poursuivis par l'exportateur de données. Toutefois, cette dérogation ne s'applique que dans un certain nombre de conditions cumulatives expressément énumérées:

- aucune des dérogations susmentionnées n'est applicable,
- le transfert n'est pas répétitif,
- le transfert ne concerne qu'un nombre limité de personnes concernées,
- le transfert est nécessaire aux fins d'intérêts légitimes impérieux poursuivis par le responsable du traitement qui ne prévalent pas sur 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, sur la base de cette évaluation, fourni 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 poursuivis, en plus de fournir les informations visées aux articles 13 et 14 du RGPD.

Pour plus d'informations:

- [Article 49 et considérants 111 à 114 du RGPD](#)
- Comité européen de la protection des données, lignes directrices 2/2018 du 25 mai 2018 sur les dérogations à l'article 49 du règlement (UE) 2016/679, disponibles à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_fr