The General Data Protection Regulation

International data transfers

Updated: 03 04 2025

Content

Introduction

EU data protection rules apply to the European Economic Area (i.e. the European Union, Liechtenstein, Norway and Iceland, hereafter the "EEA"). Personal data may therefore be transferred freely within this territory, provided that the processing complies with the general obligations applicable to controllers and processors provided for by the General Data Protection Regulation 2016/679 (the "GDPR") .

However, a transfer of personal data subject to processing to a country outside the European Economic Area (a "third country") or to an international organisation shall take place only under certain conditions as described in Chapter V of the GDPR. These requirements are additional to the general obligations provided by the "GDPR". Hence, a two-step assessment must be applied:

- first, the transfer of personal data (as a processing activity) must have a legal basis and must comply with all relevant provisions of the GDPR (e.g. lawfulness of processing, transparency, accountability, etc.);
- second, the provisions applicable to international data transfers provided for in Chapter V of the GDPR must be complied with. Thus, transfers of personal data to a third country is only possible if.
    - the data transfer is covered by an adequacy decision issued by the European Commission according to article 45 of the GDPR

      or
    - otherwise, if the data exporter can demonstrate the existence of appropriate safeguards as stated under article 46 of the GDPR

      or
    - otherwise, if the transfer falls under any of the derogations foreseen in article 49 GDPR.

Notion of "transfer of personal data to a third country"

The GDPR does not define the activities which qualify as transfer of personal data to a third country. In order to provide clarifications as to the notion of "transfer of personal data to a third country", the European Data Protection Board ("EDPB") issued Guidelines 5/2021 on the interplay between the application of Article 3 and Chapter V of the GDPR[1], setting out three cumulative criteria according to which processing would qualify as a "transfer to the third country":

1. the controller or processor is subject to the GDPR for the given processing[2],
2. the controller or processor (the "data exporter") discloses or otherwise makes personal data available to a *different* controller, joint controller or processor ("data importer")[3], and

[1] European Data Protection Board (EDPB), Guidelines 5/2021 of 18 November 2021 on the interplay between the application of Article 3 and the provisions of international transfers as per Chapter V of the GDPR.
[2] See European Data Protection Board (EDPB), Guidelines 3/2018 of 12 November 2019 on the territorial scope of the GDPR (Article 3).
[3] See section 2.2 of the above Guidelines 5/2021.

3. the importer is in a third country or is an international organisation, regardless of whether or not the GDPR is also applicable to the processing of personal data by the data importer.[4]

It should be noted that entities, which form part of the same corporate group, may qualify as separate controllers or processors and that data disclosures between such entities could be considered as transfers of personal data.[5]

The following examples constitutes "transfers" for the purpose of the GDPR[6]:

- company X established in Luxembourg, acting as controller, gives access to the personal data of its clients to a company Z established in Chile, which processes these data as processor on behalf of X,
- the Luxembourgish Company A, which is a subsidiary of the U.S. parent Company B, discloses personal data of its employees to Company B to be stored in a centralized HR database by the parent company in the U.S. In this case the Luxembourgish Company A processes (and discloses) the data in its capacity of employer and hence as a controller, while the parent company is a processor. In this case, data are provided from a controller which, as regards the processing in question, is subject to the GDPR, to a processor in a third country.

The following examples do not constitute "transfers" for the purpose of the GDPR[7]:

- the personal data are disclosed directly and on their own initiative by the data subject to the recipient. In this case, there is no controller or processor sending or making the data available, i.e. there is no "exporter",
- an employee travels to a third country and remotely access the personal data processed by the employer. The remote access of personal data from a third country by the employee does not constitute a transfer of personal data, as the employee is an integral part of the controller,
- a controller or a processor located in a third country not subject to the GDPR transmits personal data to a controller or a processor located in Luxembourg.

For more information:

- Article 3, Chapter V and Recitals (101) to (116) of the GDPR
- European Data Protection Board (EDPB), Guidelines 3/2018 of 12 November 2019 on the territorial scope of the GDPR (Article 3), available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
- European Data Protection Board (EDPB), Guidelines 5/2021 on the interplay between the application of Article 3 and the provisions of international transfers as per Chapter V of the GDPR, final version of 14.02.2023 available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en

[4] See section 2.3 of the above Guidelines 5/2021.
[5] See point 16 of the above Guidelines 5/2021.
[6] See point 18 of the above Guidelines 5/2021.
[7] *Idem.*

1. Personal data transfers to countries outside the EEA with an adequate level of protection

Controllers wishing to transfer personal data outside the EEA must first ensure that the country of destination offers an adequate level of protection.

A so-called “adequacy decision” is one of the tools provided for under the GDPR enabling transfers of personal data from the EEA to third countries (article 45 of the GDPR). More specifically, the European Commission has the power to adopt an adequacy decision, setting out that a country, a territory or one or more specified sectors within that third country, or an international organisation offers an adequate level of protection of personal data. Where such a decision has been adopted, the transfer may be carried out in the same manner as if it was carried out within the EEA[8]. The European Commission has issued adequacy decisions for the following countries:

- Andorra,
- Argentina,
- Canada (for transfers to recipients subject to the Personal Information Protection and Electronic Documents Act (“PIPEDA")),
- Faroe Islands,
- Guernsey,
- Israel,
- Isle of Man,
- Japan,
- Jersey,
- New Zealand,
- Republic of Korea,
- Switzerland ,
- United Kingdom
- United States of America (only for companies certified under the EU-US Data Privacy Framework: see next section) and
- Uruguay.

Data exporters should verify that their activities or the categories of data they are processing fall within the scope of the adequacy decision which constitutes a basis for the intended transfer.

For more information:

- Article 45 and recitals (101) – (107) of the GDPR List of third countries having an adequacy decision on the European Commission website, available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
- Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

[8] Article 45 of the GDPR.

2. Personal data transfers to the United States of America under the EU-US DPF

The European Commission adopted on 10 July 2023 an adequacy decision for the EU-US Data Privacy Framework (DPF), which replaces the Privacy Shield Framework invalidated by the Court of Justice of the European Union with the so called "Schrems II" decision[9]. As of this date, transfers from the EU to entities and organizations located in the US that are included in the 'Data Privacy Framework List' ("DPF list") may be based on the Adequacy Decision according to article 45 of the GDPR and carried out freely, without the need to rely on Article 46 GDPR transfer tools (as described in our dedicated section) or to apply supplementary measures to frame the transfers to the US.

The EU-US Data Privacy Framework introduces a system of auto-certification, which require the US entities to comply with the obligations and principles of data protection listed in this framework, such as purpose limitation and data minimisation and the respect of certain data subject rights.

This mechanism as well as the application of the legal framework of the United States of America is continuously monitored by the European Commission and the Member States of the European Union. Where the European Commission has indications that an adequate level of protection is no longer ensured, it can decide to suspend, amend or repeal the adequacy decision, or limit its scope.

For Luxembourg-based companies: under which conditions can data be transferred to the US?

Companies, associations or other organizations established in Luxembourg (or in another country in the EEA) transferring data to the US should consult the DPF website, maintained and made publicly available by the U.S. Department of Commerce ("DoC") to check whether companies to which personal data will be transferred are self-certified and comply with the framework requirements. The list of certified entities is available on the website of the US Departement of Commerce https://www.dataprivacyframework.gov/list.

It is important to note that transfers of personal data to entities in the US that are not included in the DPF list may not rely on the adequacy decision and must be carried out on the basis of one of the transfer tools under article 46(2) of the GDPR (see next section).

If the US entity receiving personal data in the US acts as a processor on behalf of the Luxembourg entity acting as controller (for example a cloud service provider), a data processing agreement under Article 28 GDPR will be required, regardless of participation of the US-company (processor) in the EU-U.S. DPF. More information on this requirement can be consulted in the section "Contract Requirements for Data Transfers to a Processor" in the FAQs – EU–U.S. Data Privacy Framework (EU–U.S. DPF) published in the US DPF official website.[10]

For Luxembourg-based data subjects: how can data subjects exercise their rights toward a certified US company or lodge a complaint against it?

[9] Court of Justice of the European Union, 16 July 2020, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems,* case C-311/18.

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

You may find more information on data subjects rights and on how to exercise them in the context of the DPF on our dedicated page [link].

For more information:

- **Adequacy decision for the EU-US Data Privacy Framework** (Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework): https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

- EDPB F.A.Q. on EU-U.S. DATA PRIVACY FRAMEWORK FOR EUROPEAN BUSINESSES adopted on 16 July 2024: https://www.edpb.europa.eu/system/files/2024-07/edpb_dpf_faq-for-businesses_en.pdf

- EDPB F.A.Q. on EU-U.S. DATA PRIVACY FRAMEWORK FOR EUROPEAN INDIVIDUALS adopted on 16 July 2024: https://www.edpb.europa.eu/system/files/2024-07/edpb_dpf_faq-for-individuals_en_0.pdf

- Questions and Answers: EU-US Data privacy framework (European Commission website): https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045

- FAQs – EU–U.S. Data Privacy Framework (EU–U.S. DPF) published in the US DPF official website: https://www.dataprivacyframework.gov/program-articles/FAQs%20%E2%80%93%20EU%E2%80%93U.S.-Data-Privacy-Framework-(EU%E2%80%93U.S.-DPF)

3. Personal data transfers to countries outside the European Economic Area without an adequate level of protection

In the absence of an adequacy decision (i.e. when a country, a territory, one or more specified sectors within that third country, or an international organisation outside the EEA is not recognised by the European Commission as offering an adequate level of protection), transfers to a third country can take place, if the data exporter has implemented "appropriate safeguards".

Article 46 of the GDPR provides for the following appropriate safeguards (or "transfer tools"):

- standard contractual clauses,
- binding corporate rules,
- codes of conduct,
- certification mechanisms and
- specific safeguards for transfers between public authorities or bodies.

It is only in the absence of such appropriate safeguards that the data exporters could use the derogations provided for in Article 49 of the GDPR[11].

[11] See section 3.5 below.

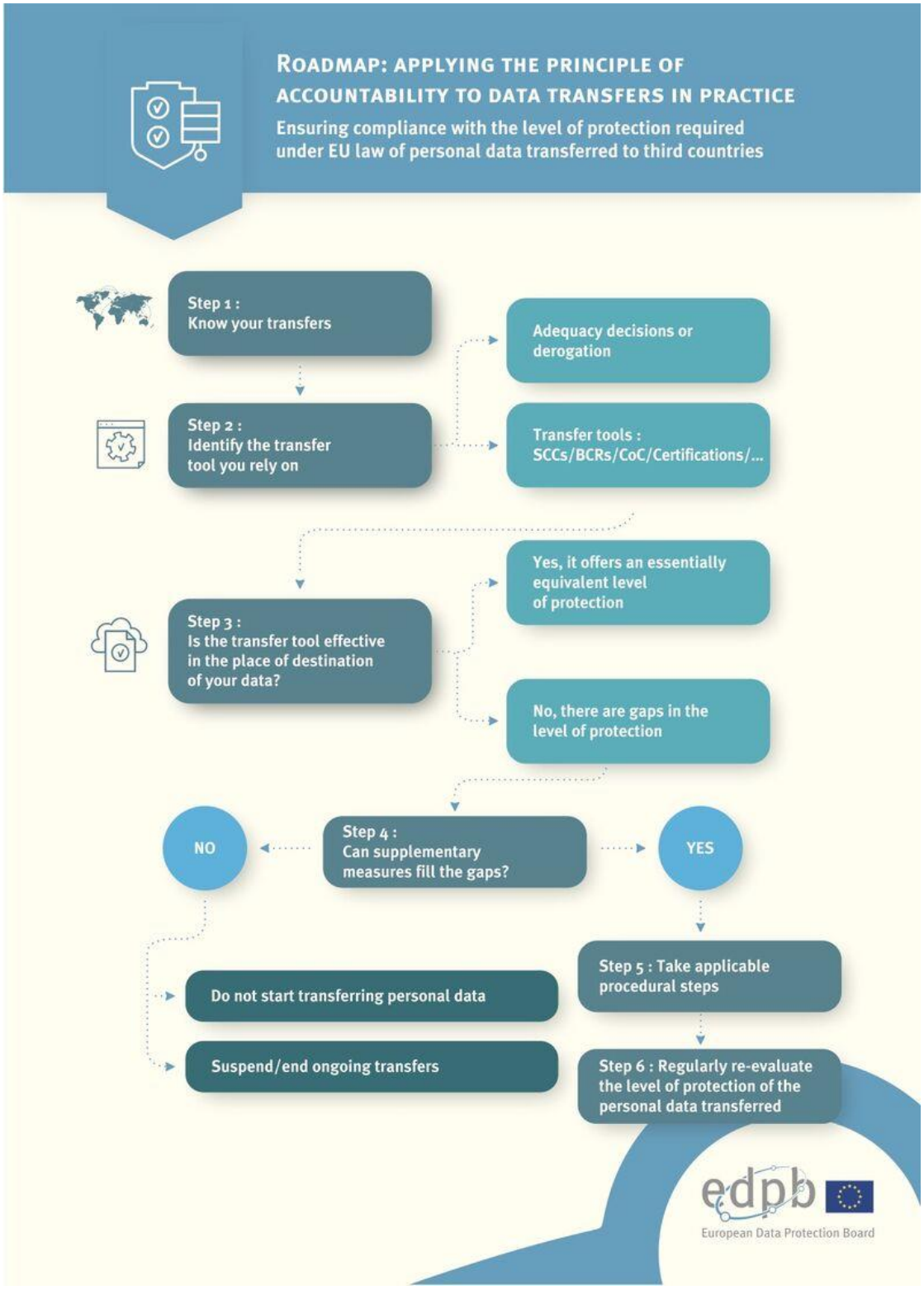
Pursuant to the principle of accountability,[12] the controller must be able to present one of the appropriate safeguards listed above on which it relies upon for the data transfer to a country outside the EEA or to an international organisation when requested to do so by the CNPD (for example, in case of a control or audit).

In this context it is important to mention, that the so called "Schrems II" judgement of the Court of Justice of the European Union[13] clarified, that it is not sufficient to demonstrate the implementation of the appropriate safeguards listed under article 46 of the GDPR. Data exporters (controllers and processors) relying on appropriate safeguards to carry out transfers of personal data to third countries must assess whether any supplementary measures to those required by the appropriate safeguards are necessary.

The data exporter needs therefore to verify, prior to any transfer, on a case-by-case basis whether the selected transfer tool or appropriate safeguard is effective in ensuring that the level of protection granted by the GDPR is not undermined by the transfer in question. In particular, the data exporter has to assess whether the legislation and/or practice in the third country to which the data is transferred may affect in practice the effectiveness of the selected transfer tool in his specific case, i.e. if it prevents the data importer to comply with its obligations provided by the transfer tool. If this so-called transfer impact assessment reveals that the selected transfer tool does not ensure in practice that the data subject are afforded a level of protection essentially equivalent to that which is guaranteed within the European Union, the data exporter has to verify, if need be with the help of the data importer, whether any supplementary measures exist (of technical, additional contractual or organisational nature), which could allow the transfer tool to be efficient to ensure an essentially equivalent level of protection to the data transferred to third countries. If such supplementary measures exist, they have to be implemented or otherwise the transfer has to be suspended and /or stopped.

The EDPB adopted Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[14], which aim to assist controllers and processors acting as data exporters with their duty to identify and implement appropriate supplementary measures. These recommendations contain a six-step approach to the transfer impact assessment, which are illustrated in the following roadmap for the assessment of the compliance of the transfers with the provisions of the article Chapter V of the GDPR.

[12] Article 5, paragraph 2 of the GDPR.
[13] Court of Justice of the European Union, 16 July 2020, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems,* case C-311/18.
[14] European Data Protection Board (EDPB), Recommendations 01/2020 of 18 June 2021 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (version 2.0).


ROADMAP: APPLYING THE PRINCIPLE OF ACCOUNTABILITY TO DATA TRANSFERS IN PRACTICE
Ensuring compliance with the level of protection required under EU law of personal data transferred to third countries
Step 1 : Know your transfers
Step 2 : Identify the transfer tool you rely on
Adequacy decisions or derogation
Transfer tools : SCCs/BCRs/CoC/Certifications/...
Step 3 : Is the transfer tool effective in the place of destination of your data?
Yes, it offers an essentially equivalent level of protection
No, there are gaps in the level of protection
Step 4 : Can supplementary measures fill the gaps?
NO
YES
Do not start transferring personal data
Suspend/end ongoing transfers
Step 5 : Take applicable procedural steps
Step 6 : Regularly re-evaluate the level of protection of the personal data transferred
edpb
European Data Protection Board

For more information:

- European Data Protection Board, Recommendations 1/2020 of 18 June 2021 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, available at: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
- European Data Protection Board, Frequently Asked Questions (FAQs) of 24 July 2020 on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, available at: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en
- Practical Guide on the Transfer impact assessment of the French data protection authority (CNIL)

3.1. Contractual Clauses

As mentioned under point 3, controllers and processors have to rely on appropriate safeguards to transfer personal data to countries outside the EEA not offering an adequate level of protection. One of the safeguards provided for by the GDPR is the use of standard contractual clauses adopted by the European Commission (article 46, paragraph 2 letter c) of the GDPR) or adopted by a supervisory authority and approved by the European Commission (article 46, paragraph 2 letter d) of the GDPR). Another safeguard is the use of so called "ad hoc" contractual clauses written by data exporters and approved by a supervisory authority, which contain sufficient safeguards to protect the transfer of personal data (article 46, paragraph 3, letter a) of the GDPR). Both standard and "ad hoc" contractual clauses are binding contracts between those who send the data (data exporters) and those who receive them (data importers).

3.1.1. Standard Contractual Clauses ("SCCs") adopted by the European Commission

Controllers and processors subject to the GDPR, including those established outside the EEA,[15] may rely on the Standard Contractual Clauses ("SCCs") issued by the European Commission.[16] [17]

The SCCs follow a modular approach to provide for a range of transfer scenarios. They contain four sets of clauses (modules) depending on the role of the data exporter and data importer as processor or controller:

- Module 1: Transfer from controller to controller("C2C"),

[15] Subject to the GDPR by virtue of Article 3 of the GDPR.
[16] European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
[17] The SCCs were updated on 4 June 2021 and replace the previously applicable SCCs.

- Module 2: Transfer from controller to processor ("C2P"),
- Module 3: Transfer from processor to processor ("P2P"),
- Module 4: Transfer from processor to controller ("P2C").

The SCCs shall be signed before any transfer takes place. Of note is that the SCCs contain a docking clause that allows additional data exporters or importers to accede to the SCCs throughout the lifecycle of the contract (Clause 7 of the SCCs).

The SCCs assist data exporters and importers in complying with the requirement of a transfer impact assessment and the implementation of supplementary measures as set out in the Schrems II judgment.

Thus, section III ("Local laws and obligations in case of access by public authorities") of the SCCs sets out that:

- the data exporter (with the assistance of the data importer) is obliged to take into account the level of protection in the third country in question, the specific circumstances of the transfer and any technical and organisational measures to put in place to supplement the SCCs, and
- the data importer has the obligation to notify the data exporter, if there are changes in the situation in the third country which create an inability to comply with the SCCs. In this case, the exporter must adopt appropriate measures to address the situation or must suspend the transfer.

Furthermore, the SCCs contain practical examples of technical supplementary measures, such as encryption.

3.1.2. "Ad hoc" Contractual Clauses

Data exporters may also rely on so-called "ad hoc clauses",[18] which may for example address the situation where personal data are initially transferred by a controller to a processor within the EU and then subsequently transferred by the processor (data exporter) to a non-EU sub processor (data importer) and subsequent sub-processors. Data exporters aiming to use ad hoc clauses must obtain an authorisation from the competent supervisory authority (for example, the CNPD) which will coordinate with other supervisory authorities in accordance with the consistency mechanism set out in Article 63 of the GDPR.[19]

In accordance with Regulation n°7/2020 of 3 April 2020 of the CNPD laying down the amount and payment terms of the fees within the framework of its powers of authorisation and consultation, each controller or processor established on the territory of Luxembourg, who submits contractual clauses for authorisation to the CNPD pursuant to Article 46, paragraph 3, letter a) of the GDPR, must pay a fee of 1.500 € to the CNPD[20].

[18] Article 46, paragraph 3, letter a) of the GDPR.
[19] Article 46, paragraph 4 of the GDPR.
[20] Available at : https://cnpd.public.lu/content/dam/cnpd/fr/decisions-avis/2020/07-2020-reglement-CNPD-redevances-signe.pdf.

For more information:

- Article 46 and recitals (108), (109) and (114) of the GDPR
- Standard contractual clauses adopted by the European Commission:
    - European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
    - European Commission, Questions and Answers of 25 May 2022 for the Standard Contractual Clauses, available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en Article 29 Working Party, Working document 01/2014 of 21 March 2014 on Draft « ad hoc » contractual clauses "EU processor to non-EU sub-processor" (« P-to-P ») (WP214), available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf

3.2. Binding Corporate Rules ("BCRs")

In the absence of an adequacy decision, data exporters may rely on Binding Corporate Rules ("BCRs"), which are designed to allow groups of companies and multinational organisations to transfer personal data from the EEA to affiliate entities located outside the EEA in compliance with Chapter V of the GDPR.[21]

BCRs are internal rules adopted by a group of companies, which set out its global policy for international transfers of personal data. These rules must be binding and complied with by all group entities, regardless of their countries of establishement, as well as by all their employees. Moreover, they must expressly confer enforceable rights to data subjects with regard to the processing of their personal data.

There exist two different types of BCRs. The choice of the correct type of the BCR is important since they cover different situations which are subject to different requirements to the content of the BCRs as specified by article 47 GDPR.

The Controller BCRs cover transfers from a group entity established in the EEA and acting as a controller to another group entity established in the third country which is acting as a controller, a processor or a sub-processor. More information on the scope and the requirements in the BCR for Controllers can be found in the EDPB Referential for Controllers BCR, adopted on 20 June 2023.[22]

The Processor BCRs cover transfers from a group entity established in the EEA and acting as a processor for an external controller to another group entity as sub-processor. More information on the scope and requirements in the BCR for Processors can be found in the amended Working

[21] Articles 46, paragraph 2, and 47 of the GDPR.
[22] EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules.

Document of the Article 29 Working Party (WP29) on Binding Corporate Rules for Processors (wp257rev).[23]

The BCRs are approved by the competent supervisory authority, which coordinates with other supervisory authorities in accordance with the consistency mechanism set out in Article 63 of the GDPR.

Approval process for BCRs

The procedure for approving binding corporate rules (BCRs) for controllers and processors is laid out under Articles 47 (1), 63, 64 and (where necessary) 65 of the GDPR.

The approval process for BCR's consists of the following steps[24]:

1. identification of the lead supervisory authority for the approval of the BCRs,
2. cooperation procedure for the approval of BCRs between the lead supervisory authority the supervisory authorities acting as co-reviewers and the other concerned supervisory authorities,
3. adoption of the EDPB opinion,[25]
4. issuing of a national decision by the lead supervisory authority, taking into account the EDPB's opinion.

In accordance with Article 6 of the Regulation n°7/2020 of 3 April 2020 of the CNPD[26] laying down the amount and payment terms of the fees within the framework of its powers of authorisation and consultation, each group of undertakings established on the territory of Luxembourg, who submits binding corporate rules to the CNPD for approval pursuant to Article 47 of the GDPR, must pay a fee of 1.500 € to the CNPD.

For more information:

- Information on Binding Corporate Rules on the European Commission's website, available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en
- EDPB Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority available at: https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202208_identifying_lsa_targeted_update_v2_en.pdf

23 Working Document on Binding Corporate Rules for Processors (wp257rev.01) :https://ec.europa.eu/newsroom/article29/items/614110

24 Articles 47, paragraph 1, 63 and 64, paragraph 1, letter f) of the GDPR and Article 29 Working Party, Working Document of 11 April 2018 setting forth a co-operation procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR (WP263rev.01),, endorsed by the European Data Protection Board on 25 May 2018.

25 In accordance with Article 64, paragraph 3 of the GDPR.

26 Available at : https://cnpd.public.lu/content/dam/cnpd/fr/decisions-avis/2020/07-2020-reglement-CNPD-redevances-signe.pdf.

- Woking document on the approval procedure of the Binding Corporate Rules for controllers and processors (wp263rev.01), available at: https://ec.europa.eu/newsroom/article29/items/623056/en
- BCR Referential for Controllers, adopted on 20 June 2023 (Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules), available at : https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-12022-application-approval-and_en
- Working Document on Binding Corporate Rules for Processors (wp257rev.01): https://ec.europa.eu/newsroom/article29/items/614110
- Recommendation on the standard application form for the approval of the Processor Binding Corporate Rules form (wp265): https://ec.europa.eu/newsroom/article29/items/623848/en

3.3. Codes of conduct

In the absence of an adequacy decision, data exporters (controllers and processors) may rely on approved codes of conducts[27] as appropriate safeguards for transfers of personal data to third countries.

Codes of conduct are typically drafted by entities, associations or federations that represent large categories of controllers and processors, such as industry-specific associations or trade unions.

Codes of conduct must be approved by the competent supervisory authority and comply with the specific requirements in articles 40 and article 46 (2) e) of the GDPR and the EDPB Guidelines 04/2021[28] on Codes of Conduct as tools for transfers in order to constitute appropriate safeguards within the framework of transfers of personal data to third countries or international organisations.

Once approved by the competent supervisory authority, a Code of conduct may be adhered to by data exporters (controllers or processors). In addition, those exporters must thus provide binding and enforceable commitments to confirm that said Code of conduct ensures appropriate safeguards for transfers of data outside of the EEA.[29]

Further information can be found in the EDPB Guidelines 01/2019 on Codes of Conduct and monitoring Bodies as well as in the EDPB Guidelines 04/2021 on Codes of Conduct as tools for transfers.

For more information:

- Articles 40, 41 and 46 and recitals (98), (99) and (114) of the GDPR.
- Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, adopted on 4 June 2019: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en

[27] Article 46, paragraph 2, letter e) of the GDPR.
[28] EDPB Guidelines 1/2019 of 4 June 2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.
[29] Articles 40, paragraphs 3 and 9, and 46, paragraph 2, letter e) of the GDPR.

- European Data Protection Board, Guidelines 04/2021 of 22 February 2022 on Codes of Conduct as tools for transfers, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_en

3.4. Certification mechanisms

In the absence of an adequacy decision, data exporters (controllers and processors) may rely on certifications mechanisms as appropriate safeguards for transfers of personal data to third countries.[30] Certification mechanisms may be developed and established to demonstrate the existence of appropriate safeguards provided by data importers (controllers or processors) in third countries in order to allow for personal data transfers to third countries.[31] Certified third-country data importers (controllers or processors) shall in addition to the certification make binding and enforceable commitments, via contractual of other legally binding instruments, to apply the safeguards upon which the certification is based on[32].

Certification mechanisms must be approved by the competent supervisory authority and comply with articles 42 and 46 (2) f) of the GDPR[33] as well as with the EDPB Guidelines 07/2022 on certification as a tool for transfers[34] in order to constitute appropriate safeguards within the framework of transfers of personal data to third countries or international organisations. Further information can be found in the EDPB Guidelines 07/2022 on certification as a tool for transfers. These guidelines provide guidance on specific aspects regarding certification as a tool for transfers, such as the purpose, scope and the different actors involved. Furthermore, they contain specific requirements for accreditation of a certification bodies andspecific certification criteria for the purpose of demonstrating the existence of appropriate safeguards for transfers. Finally, they clarify the elements that should be addressed in the binding and enforceable commitments that data importers (controllers or processors) in the third country not subject to the GDPR should take for the purpose of providing appropriate safeguards to data transferred to third countries.

Certification as a tool transfer can cover transfers from all EU countries (EU-Seal) or just transfers from one EU member state to the third countries (national certification). In the latter case, the national authority approves the certification mechanism following an EDPB opinion. In case of an EU-Seal, the EDPB approves the certification mechanism. Once the certification as tool for transfers is approved, data importers form third countries can apply for certification with certification bodies. Data exporters transferring data to certified data importers can then rely on the certification mechanism as an appropriate safeguard.

Further information on the approval procedure can be found in the EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation.

In accordance with article 4 of the Regulation n°7/2020 of 3 April 2020 of the National Data Protection Commission laying down the amount and payment terms of the fees within the framework of its powers of authorisation and consultation, each scheme owner, who submits to

[30] Article 46, paragraph 2, letter f) of the GDPR.
[31] Articles 42 and 46, paragraph 2, letter f) of the GDPR.
[32] Article 42, paragraph 2 of the GDPR.
[33] See Articles 40, 42 and 46 of the GDPR.
[34] EDPB Guidelines 07/2022 of 14 February 2023 on Certification as tool for transfers.

the CNPD an application for approval of a certification scheme pursuant to Article 42 (5) of the GDPR, must pay a fee to the CNPD the amount of which depends on the step of the procedure.

For more information:

- Articles 42,43 and 46 and recitals (100) and (114) of the GDPR.
- European Data Protection Board, Guidelines 1/2018 of 4 June 2019 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en
- European Data Protection Board, Guidelines 4/2018 of 4 June 2019 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679), available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en
- Guidelines 07/2022 on Certification as tool for transfers, adopted on 14 February 2023: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_en

3.5. Specific safeguards for transfers between public authorities or bodies

Transfers from a public authority or body in the EEA to another public authority or body in a third country may take place:

- with a legally binding and enforceable instrument between public authorities or bodies, without requiring a prior authorisation from the CNPD,[35] or
- if a public authority or body does not have the power to enter into legally binding and enforceable arrangements, through administrative arrangements, which may be concluded between public authorities or bodies and which provide for enforceable and effective data subject rights and effective legal remedies, with a prior authorisation from the CNPD in accordance with the consistency mechanism set out in Article 63 of the GDPR.[36]

For more information:

- European Data Protection Board, Opinion 4/2019 of 12 February 2019 on the draft AA between EEA and non-EEA Financial Supervisory Authorities, available at: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-42019-draft-aa-between-eea-and-non-eea_en
- European Data Protection Board, Guidelines 2/2020 of 15 December 2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA

[35] Article 46, paragraph 2, letter a) of the GDPR.
[36] Article 46, paragraphs 3, letter b), and 4) of the GDPR.

and non-EEA public authorities and bodies, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en

– European Data Protection Board, 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, available at: https://edpb.europa.eu/our-work-tools/our-documents/toolbox-essential-data-protection-safeguards-enforcement-cooperation_en

4. Derogations for specific situations

Article 49 of the GDPR lists exhaustively a certain number of derogations. Those are exemptions from the general principle that personal data may only be transferred to third countries, if an adequate level of protection is provided for in the third country or if appropriate safeguards have been adduced as described in the previous sections.

These derogations shall therefore only be used in specific situations as listed below. If it is not possible to rely on any adequacy decision or appropriate safeguard. It is only in the absence thereof that controllers or processors could use one of the derogations set out in the GDPR. When relying on derogations, controllers should be able to demonstrate why it was not possible to rely on appropriate safeguards, as required by the 'accountability' principle.

Based on the derogations, the personal data can be transferred to a third country where:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

As a « last resort » derogation, personal data can be transferred if it is necessary for the purposes of the compelling legitimate interests pursued by the data exporter. However, this derogation only applies under a number of specific, expressly enumerated cumulative conditions:

- none of the above-mentioned derogations is applicable,
- the transfer is not repetitive,
- the transfer concerns only a limited number of data subjects,
- the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject,
- the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data,
- the controller has informed the supervisory authority (e.g. the CNPD) of the transfer, and
- the controller has informed the data subject of the transfer and on the compelling legitimate interests pursued, in addition to providing the information referred to in articles 13 and 14 of the GDPR.

For more information:

- Article 49 and recitals (111) – (114) of the GDPR
- European Data Protection Board, Guidelines 2/2018 of 25 May 2018 on derogations of Article 49 under Regulation 2016/679, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en