



The General Data Protection Regulation

International data transfers

Content

Introduction.....	3
1. Transfers within the European Economic Area (European Union, Liechtenstein, Norway and Iceland)	3
2. Transfers outside the European Economic Area with adequate protection	3
2.1. The “EU-U.S. Privacy Shield Framework”	4
3. Transfers outside the European Economic Area without adequate protection	5
3.1. Contractual clauses	5
3.1.1. Standard data protection clauses	5
3.1.2. “Ad hoc” clauses	6
3.2. Binding Corporate Rules (BCRs)	6
3.3. Codes of conduct and certification mechanisms.....	8
3.4. Specific safeguards for transfers between public authorities or bodies	8
3.5. Derogations for specific situations	8
4. International cooperation in the field of Police and Justice.....	10

Introduction

Any transfer of personal data, which are undergoing processing or which will be processed after the transfer, to a country outside the European Economic Area (i.e. European Union, Liechtenstein, Norway and Iceland) (the “EEA”) or to an international organisation shall take place only under certain conditions.

These conditions are additional to the [obligations applicable to controllers and processors](#). Hence, a two-step test must be applied:

- firstly, the processing must have a legal basis and must comply with all relevant provisions of the GDPR (e.g. lawfulness of processing, compatibility of the communication of data to a third party with the initial processing activity, information to the data subjects);
- secondly, the provisions applicable to international data transfers must be complied with.

More information:

- [Chapter V of the General Data Protection Regulation](#)

1. Transfers within the European Economic Area (European Union, Liechtenstein, Norway and Iceland)

EU data protection rules apply to the European Economic Area and personal data may therefore be transferred freely between these countries, provided that the processing complies with the general principles of the GDPR (e.g. lawfulness of processing, compatibility of the communication of data to a third party with the initial processing activity, information to the data subjects).

More information:

- [Obligations applicable to controllers and processors in the EEA](#)
- Guidance on the consequences of Brexit on international data transfers.

2. Transfers towards a country outside the European Economic Area with an adequate level of protection

Any controller wishing to transfer personal data outside the EEA must first ensure that the country of destination offers an adequate level of protection. If the level of protection of the destination country can be considered adequate, the personal data may be transferred in the same manner as if they were transferred within the EEA.

The general principles of the GDPR (e.g. lawfulness of processing, compatibility of the communication of data to a third party with the initial processing activity, information to data subjects) must, in all circumstances, be observed.

The European Commission is authorised to decide 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, and has done so for the following countries:

- Andorra;
- Argentina;
- Canada (*only for commercial organisations subject to the Canadian « Personal Information Protection and Electronic Documentation Act »*);
- the Faroe Islands;
- Guernsey;
- Israel;
- Isle of Man;
- Japan (*only for personal information handling business operators subject to the Japanese “Act on the Protection of Personal Information” as complemented by the “Supplementary Rules set”*);
- Jersey;
- New Zealand;
- Switzerland;
- Uruguay; and
- the United States of America (*limited to the « EU-U.S. Privacy Shield Framework »*).

Adequacy talks are also ongoing between the European Commission and South Korea.

More information:

- [List of third countries subject to an adequacy decision of the European Commission](#)

2.1. The “EU-U.S. Privacy Shield Framework”

The so-called “EU-U.S. Privacy Shield Framework” (operational since 1 August 2016) protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States of America for commercial purposes. The framework also brings legal clarity for businesses relying on transatlantic data transfers. It is intended to reflect the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old “Safe Harbour framework” invalid.

It consists of Privacy Principles that companies must abide by and commitments on how the arrangement will be enforced. More specifically, U.S. companies can register to be on the Privacy Shield list and self-certify that they meet the high data protection standards set out by the arrangement. They have to renew their registration every year. The U.S. Department of Commerce monitors and verifies that companies' privacy policies are in line with the relevant Privacy Shield principles and are readily available to the public.

More information :

- [List of U.S. companies registered on the Privacy Shield list](#)
- [The “EU-US Privacy Shield Framework” on the European Commission’s website](#)

- [The “EU-U.S. Privacy Shield Framework” dedicated website \(U.S. Department of Commerce\)](#)
- [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. Transfers towards a country outside the European Economic Area without an adequate level of protection

When a country outside the EEA is not recognised by the European Commission as offering an adequate level of protection, there are several options that can be used to transfer personal data to these countries.

The CNPD recommends, as its EU counterparts, a layered approach to transfers consisting of considering first whether the third country provides an adequate level of protection and ensuring that the exported data will be safeguarded in the third country. If there is no adequacy decision, data exporters should first endeavour to apply **appropriate safeguards** provided for by Articles 45 and 46 of the GDPR (contractual clauses, binding corporate rules, codes of conduct, certification mechanisms, or specific safeguards for transfers between public authorities or bodies) to the transfer. It is only in the absence of such guarantees that the data exporters should use the **derogations** provided for in Article 49 of the GDPR.

3.1. Contractual clauses

Data exporters can use a series of appropriate safeguards enabling transfers to countries not offering an adequate level of protection. One of these safeguards is the possibility for controllers to offer adequate protection through a contract, which is binding for those who send the data and those who receive them, and which contains sufficient safeguards to protect the personal data.

3.1.1. Standard data protection clauses

To help controllers, the European Commission has adopted standard contractual clauses (or “model contracts”) that are considered to offer sufficient safeguards in light of the applicable data protection rules.

The following standard data protection clauses may be used without an authorisation from the CNPD:

- [Clauses for the transfer from a EU/EEA controller to a non-EU/non-EEA controller \(« C-to-C », first set, as annexed in the European Commission’s decision 2001/497/EC\)](#)
- [Clauses for the transfer from a EU/EEA controller to a non-EU/non-EEA controller \(« C-to-C », second set, as annexed in the European Commission’s decision 2004/915/EC\)](#)

- [Clauses for the transfer from a EU/EEA controller to a non-EU/non-EEA processor \(« C-to-P », as annexed in the European Commission's decision 2010/87/EU\)](#)

The controller or processor should always be able to present its standard data protection clauses when requested so by the CNPD (for example, in case of a control or audit).

More information:

- [Model contracts for the transfer of personal data to third countries, on the European Commission's website](#)
- [F A Q adopted by the Article 29 Data Protection Working Party \(predecessor of the EDPB\) on "C-to-P" clauses \(WP176\)](#)

3.1.2. "Ad hoc" clauses

If controllers or processors do not use for the European Commission's standard contractual clauses, they can draft their own contractual clauses ("ad hoc" clauses) offering sufficient data protection safeguards. These clauses must be submitted to the CNPD in accordance with Article 46 (3) (a) of the GDPR. These clauses will subsequently have to be approved by the European Data Protection Board in accordance with Article 46 (4) of the GDPR through the consistency mechanism.

More information:

- [Model of draft « ad hoc » contractual clauses "EU data processor to non-EU sub-processor" \(« P-to-P »\), adopted by the Article 29 Data Protection Working Party \(predecessor of the EDPB\) \(WP214\)](#)

3.2. Binding Corporate Rules ("BCRs")

Binding Corporate Rules ("BCRs") help ensure an adequate level of protection for data exchanged within a group of companies located both inside and outside the European Economic Area, and are ideal for a multinational group of companies that carries out a large number of international data transfers.

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 respected by all group entities, regardless of their host countries, as well as by all their employees. Moreover, they must expressly confer enforceable rights on data subjects with regard to the processing of their personal data.

BCRs offer many advantages for a multinational group of companies by:

- aiding compliance with the General Data Protection Regulation (Article 47),

- reducing the need for appropriate safeguards for each individual transfer (for example, by adopting BCRs on a group level, data exporters would not be required to sign as many standard contractual clauses as there are transfers);
- harmonising practices relating to the protection of personal data within a group,
- providing an internal guide for employees with regard to the personal data management, as part of the 'accountability' principle,
- communicating externally on the company's data protection policy,
- to consider data protection as part of the group's corporate social responsibility.

Approval process for BCRs

The procedure for approving binding corporate rules (BCRs) for controllers and processors is laid out in Articles 47 (1), 63, 64 and (where necessary) 65 of the GDPR, and further described in the Working Document WP263 rev.01 adopted on 11 April 2018 by the "Article 29" Data Protection Working Party (predecessor of the European Data Protection Board).

It consists of the following steps:

- identification of the BCRs lead supervisory authority,
- cooperation procedure for the approval of BCRs between the lead supervisory authority, the "co-reviewers" supervisory authorities and the other concerned supervisory authorities,
- (non-binding) opinion adopted by the EDPB in accordance with Article 64 (3) of the GDPR,
- approval (or not) of the BCRs by the lead supervisory authority, taking into account the EDPB's opinion.

More information:

- [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 \(WP 257 rev.01\)](#)
- [Approval of binding corporate rules on the European Commission's website](#)
- [Procedure for BCRs application on the Belgian Data Protection Authority's website](#)

3.3. Codes of conduct and certification mechanisms

Since the entry into force of the GDPR on 25 May 2018, new transfer mechanisms are available to controllers or processors, who intend to transfer personal data to a third country with no adequate level of protection. These are:

- approved codes of conduct pursuant to Article 40 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights, and
- approved certification mechanisms pursuant to Article 42 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

More information:

- [Article 46 of the General Data Protection Regulation](#)
- [EDPB, 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. Specific safeguards for transfers between public authorities or bodies

Transfers from a Luxembourg public authority or body to another public authority or body in a third country (i.e. outside the European Economic Area) may take place:

- with a legally binding and enforceable instrument between public authorities or bodies, without requiring any specific authorisation from the CNPD, or
- with provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights. These provisions have to be submitted to the CNPD according to Article 46 (3) (b) of the GDPR and subsequently these clauses will have to be approved by the European Data Protection Board in accordance with Article 46 (4) of the GDPR through the consistency mechanism.

More information:

- [Article 46 of the General Data Protection Regulation](#)

3.5. Derogations for specific situations

Derogations under Article 49 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 and the data subjects enjoy enforceable and effective rights in order to continue to benefit from their fundamental rights and safeguards.

These derogations shall therefore only be used in specific situations: controllers or processors should first endeavour to apply one of the above-mentioned appropriate safeguards. Only in the absence of such appropriate safeguards, can controllers or processors use one of the derogations set out in Article 49 of the GDPR, and 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 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 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.

More information:

- [Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted by the EDPB on 25 May 2018](#)
- [Article 49 of the General Data Protection Regulation](#)

4. International cooperation in the field of Police and Justice

Transfers of personal data may take place between different countries in the context of international cooperation in the field of Police and Justice, in accordance with existing international agreements or treaties. Cross-national supervisory authorities (e.g. Europol, Eurojust) apply data protection principles in the context of their activities.

The European Union has signed bilateral passenger name record (PNR) agreements with the United States of America, Canada and Australia. PNR data is information provided by passengers when they book tickets and when checking in for flights, as well as data collected by air carriers for their own commercial purposes. PNR data can be used by law enforcement authorities to fight serious crime and terrorism. The transfer of PNR data from the EU to third countries can only be done through a bilateral agreement that provides for a high level of personal data protection.

The European Union has also signed a bilateral agreement with the United States of America regarding the transfer of financial data, called “Terrorist Finance Tracking Programme” (TFTP).

More information:

- [Transfer of air passenger name record data and terrorist finance tracking programme on the European Commission’s website](#)
- [Article 50 of the General Data Protection Regulation](#)