

**Procedure for International**

**Transfers of Personal Data**

**Contents**

[1 Introduction 8](#_Toc485995568)

[2 Procedure for International Transfers of Personal Data 9](#_Toc485995569)

[2.1 Determine the destination country or countries 9](#_Toc485995570)

[2.2 Establish whether an adequacy decision applies 9](#_Toc485995571)

[2.3 Implement appropriate safeguards 10](#_Toc485995572)

[2.3.1 Binding Corporate Rules 10](#_Toc485995573)

[2.3.2 Standard Data Protection Clauses 11](#_Toc485995574)

[2.3.3 Codes of Conduct 11](#_Toc485995575)

[2.3.4 Certification Schemes 11](#_Toc485995576)

[2.4 Other acceptable conditions for transfers of personal data 11](#_Toc485995577)

[2.5 Exceptional Transfers 12](#_Toc485995578)

[2.6 Putting the Transfer in Place 12](#_Toc485995579)

# Introduction

This procedure is intended to be used when putting in place a new arrangement for the transfer of personal data to a country outside of the European Union or to an international organization. It may also be used when validating whether existing arrangements meet the requirements of the General Data Protection Regulation (GDPR).

An international organization is defined by the GDPR as *“an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries” (GDPR Article 4).*

The intention of the GDPR is to protect the personal data of EU citizens wherever it is held; there are strict requirements governing where personal data can be transferred to and the measures that must be in place for such as transfer to be legal. The penalties for contravening the GDPR are significant and care must be taken by to ensure that we remain within the law at all times.

This procedure should be considered in conjunction with the following related documents:

* *Data Protection Impact Assessment Process*
* *Privacy and Personal Data Protection Policy*
* *Data Subject Request Procedure*

# Procedure for International Transfers of Personal Data

## Determine the destination country or countries

In order to establish whether a transfer of personal data is legal under the GDPR, the destination country or countries must be firmly established, along with any other countries that will receive an onward transfer of the personal data as part of the arrangement.

This may also involve reaching a clear understanding of the legal basis of any international organizations that will be receiving the personal data, in particular the countries that are part of the agreement governing those organizations.

## Establish whether an adequacy decision applies

Once a clear understanding of the destination country or countries of the personal data has been established, the list of countries and international organizations for which an adequacy decision applies must be consulted. This list is published in the *Official Journal of the European Union* and on the European Commission website (ec.europa.eu).

[Note: currently the list of countries subject to an adequacy decision may be found at

<http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>

and is as follows: Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay

An adequacy decision means that the European Commission considers the level of protection for personal data in that country to be acceptable and therefore transfers do not require any additional legal safeguards to be put in place. Adequacy decisions are regularly reviewed, at least every four years and can be repealed in the event that the EC no longer considers that the country in question meets their requirements for protection of personal data.

A special case in this area is that of the EU-US Privacy Shield which covers transfers of the personal data of EU citizens to the USA. US organizations that sign up to the Privacy Shield may store and process such personal data as long as they meet strict safeguards that are equivalent to the requirements of the GDPR. Personal data may effectively be transferred to such US organizations as if an adequacy decision applied.

[Note: the list of organizations that are active in the EU-US Privacy Shield is here –

<https://www.privacyshield.gov/list> ]

## Implement appropriate safeguards

In the event that the country or one or more of the countries to which personal data is to be transferred is not subject to an adequacy decision from the EC, appropriate safeguards must be put in place to provide for data subjects’ rights and enforceable legal remedies.

There are a number of ways in which the GDPR allows for these safeguards to be provided. These are:

1. between public authorities or bodies only, via a legally binding agreement which is capable of being enforced
2. using binding corporate rules
3. using standard data protection clauses adopted either by the European Commission or the relevant supervisory authority
4. via an approved code of conduct
5. via a certification scheme

The status of some of the above safeguards may change over time, as the GDPR becomes more mature and further guidance is issued both by the European Commission and the individual supervisory authorities.

The most appropriate method of providing protection for the rights of data subjects whose data will be transferred should be chosen and incorporated into the contractual clauses of the relevant agreement.

### Binding Corporate Rules

The supervisory authority that is relevant to the transfer (usually in the country of the controller of the data) has the power to approve a set of binding corporate rules (BCRs) that may be used to cover the transfer of personal data from a data protection viewpoint.

These binding corporate rules are required by the GDPR to specify all aspects of the transfer, including how data protection will be provided, how data subjects will exercise their rights and how compliance will be verified. The full requirements are listed in *Article 47 (“Binding corporate rules”)* paragraph 2, points a) to n) of the GDPR.

The initial creation and approval (by the supervisory authority) of BCRs is a significant piece of work that must be approached with the full commitment of the senior management of and may take a long time to achieve (more than twelve months is not uncommon). There may be an existing set of BCRs that may apply to the transfer being considered and advice should be sought from the legal department if it is intended to use this route to comply with the GDPR with regard to a data transfer.

### Standard Data Protection Clauses

The European Commission and each of the individual supervisory authorities may create and maintain sets of model data protection clauses that are intended to be used in contracts that apply to the transfer of personal data. When used in their entirety, these clauses are generally accepted as meeting the requirements of the GDPR to provide adequate safeguards.

To obtain the latest version of these clauses, refer to the website of the relevant supervisory authority.

### Codes of Conduct

Article 40 of the GDPR *(“Codes of conduct”)* provides for the drawing up of appropriate codes of conduct by organizations such as associations and industry bodies to address compliance with the GDPR. Organizations then agree to abide by the code of conduct and their compliance is monitored by the relevant association.

Such a code of conduct may be used to cover an international transfer of personal data and whether has already, or could, sign up to such a code, may be investigated as a possible route to provide appropriate safeguards.

### Certification Schemes

Certification to an approved scheme may also be used to demonstrate that appropriate safeguards are in place to protect the transfer of personal data internationally. This will apply to both the sender and recipient of the data and will require that an approved certification scheme is available in the country of the recipient.

## Other acceptable conditions for transfers of personal data

In the event that an adequacy decision does not apply to the destination country and appropriate safeguards cannot be put in place via the above methods, a transfer of personal data may only be made internationally if ***one*** of the following situations applies:

1. the data subject explicitly consents to the transfer, having been informed of the risks
2. the transfer is necessary to meet contractual commitments to the data subject or the data subject asks for the transfer prior to contract
3. the transfer is in the data subject’s interests with regard to a contract
4. it is for important reasons of public interest (recognized by law)
5. the transfer is to do with a legal claim
6. the data subject’s vital interests are protected by the transfer or if they are unable to consent
7. the transfer is made from a public register

The specifics of each of these conditions must be reviewed directly from the *GDPR Article 49 (“Derogations for specific situations”)* before basing a transfer on them.

## Exceptional Transfers

If none of the conditions set out in this procedure apply then an international transfer of personal data may only take place if ***all*** of the following conditions apply:

1. The transfer is not repetitive
2. A limited number of data subjects is involved
3. It is for compelling legitimate interests which are not overridden by those of the data subject
4. All of the circumstances of the data transfer have been assessed
5. Suitable safeguards are provided, based on the assessment
6. The assessment and the safeguards are documented
7. The supervisory authority is informed of the transfer
8. The data subject is informed of the data transfer and the reasons for it
9. The data subject is informed about his/her rights under the GDPR

Refer to *GDPR Article 49 (“Derogations for specific situations”) paragraph 1* for the exact definitions of the above conditions.

## Putting the Transfer in Place

Once the legal basis of the transfer of personal data has been established and approved, the mechanics of achieving the transfer should be addressed. These will vary according to factors such as the type and volume of data involved, the destination and the technology used.

Care must be taken to ensure that the safeguards that have been agreed to as part of the setting up of the transfer are adhered to and that evidence of their use is maintained for future audit purposes.

The website of the European Commission and the relevant supervisory authority should be monitored so that any changes that affect the legality or performance of the transfer are identified and acted upon.