

International transfers

At a glance

- The GDPR primarily applies to controllers and processors located in the European Economic Area (the EEA) with some exceptions.
- Individuals risk losing the protection of the GDPR if their personal data is transferred outside of the EEA.
- On that basis, the GDPR restricts transfers of personal data outside the EEA, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.
- A transfer of personal data outside the protection of the GDPR (which we refer to as a 'restricted transfer'), most often involves a transfer from inside the EEA to a country outside the EEA.
- If you wish to do so, you should answer the following questions, until you reach a provision which permits your restricted transfer:

1. Are we planning to make a restricted transfer of personal data outside of the EEA?

If no, you can make the transfer. If yes go to Q2

2. Do we need to make a restricted transfer of personal data in order to meet our purposes?

If no, you can make the transfer without any personal data. If yes go to Q3

3. Has the EU made an 'adequacy decision' in relation to the country or territory where the receiver is located or a sector which covers the receiver?

If yes, you can make the transfer. If no go to Q4

4. Have we put in place one of the 'appropriate safeguards' referred to in the GDPR?

If yes, you can make the transfer. If no go to Q5

5. Does an exception provided for in the GDPR apply?

If yes, you can make the transfer. If no you cannot make the transfer in accordance with the GDPR

- If you reach the end without finding a provision which permits the restricted transfer, you will be unable to make that restricted transfer in accordance with the GDPR.

In brief

What are the restrictions on international transfers?

The GDPR restricts the transfer of personal data to countries outside the EEA, or international



organisations. These restrictions apply to all transfers, no matter the size of transfer or how often you carry them out.

In more detail - European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state and each EEA state. It adopts guidelines for complying with the requirements of the GDPR.

The EDPB is currently working on its guidance in relation to International Transfers, and we will update our guide as this is published.

Further Reading

 [Relevant provisions in the GDPR – see Article 44 and Recitals 101-102](#) 

External link

Are we making a transfer of personal data outside the EEA?

1) Are we making a restricted transfer?

You are making a restricted transfer if:

- the GDPR applies to your processing of the personal data you are transferring. The scope of the GDPR is set out in Article 2 (what is processing of personal data) and Article 3 (where the GDPR applies). Please see the section of the guide [What is personal data](#). We will be providing guidance on where the GDPR applies later this year. In general, the GDPR applies if you are processing personal data in the EEA, and may apply in specific circumstances if you are outside the EEA and processing personal data about individuals in the EEA;
- you are sending personal data, or making it accessible, to a receiver to which the GDPR does not apply. Usually because they are located in a country outside the EEA; and
- the receiver is a separate organisation or individual. The receiver cannot be employed by you or by your company. It can be a company in the same group.

Example

A UK company uses a centralised human resources service in the United States provided by its parent company. The UK company passes information about its employees to its parent company in connection with the HR service. This is a restricted transfer.

Example

A UK company sells holidays in Australia. It sends the personal data of customers who have bought the holidays to the hotels they have chosen in Australia in order to secure their bookings. This is a restricted transfer.

Transfer does not mean the same as transit. If personal data is just electronically routed through a non-EEA country but the transfer is actually from one EEA country to another EEA country, then it is not a restricted transfer.

Example

Personal data is transferred from a controller in France to a controller in Ireland (both countries in the EEA) via a server in Australia. There is no intention that the personal data will be accessed or manipulated while it is in Australia. Therefore the transfer is only to Ireland.

You are making a restricted transfer if you collect information about individuals on paper, which is not ordered or structured in any way, and you send this to a service company located outside of the EEA, to:

- put into digital form; or
- add to a highly structured manual filing system relating to individuals.

Example

A UK insurance broker sends a set of notes about individual customers to a company in a non-EEA country. These notes are handwritten and are not stored on computer or in any particular order. The non-EEA company adds the notes to a computer customer management system. This is a restricted transfer.

Putting personal data on to a website will often result in a restricted transfer. The restricted transfer takes place when someone outside the EEA accesses that personal data via the website.

If you load personal data onto a UK server which is then available through a website, and you plan or anticipate that the website may be accessed from outside the EEA, you should treat this as a restricted transfer.

2) Is it to a country outside the EEA?

The EEA countries consist of the EU member states and the EFTA States.

The EU member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom.

The **EEA** states are Iceland, Norway and Liechtenstein. The EEA Joint Committee has made a decision that the GDPR applies to those countries and transfers to those countries are not restricted.

Further Reading

 [Relevant provisions in the GDPR - see Article 44 and Recital 101](#) 

External link

Do we need to make a restricted transfer of personal data to outside the EEA?

Before making a restricted transfer you should consider whether you can achieve your aims without actually sending personal data.

If you make the data anonymous so that it is never possible to identify individuals (even when combined with other information which is available to receiver), it is not personal data. This means that the restrictions do not apply and you are free to transfer the anonymised data outside the EEA.

Further Reading

 [Relevant provisions in the GDPR – see Article 44 and Recital 26](#) 

External link

How do we make a restricted transfer in accordance with the GDPR?

You must work through the following questions, in order.

If by the last question, you are still unable to make the restricted transfer, then it will be in breach of the GDPR.

Has the EU Commission made an ‘adequacy decision’ about the country or international organisation?

If you are making a restricted transfer then you need to know whether it is covered by an EU Commission “adequacy decision”.

This decision is a finding by the Commission that the legal framework in place in that country, territory or sector provides ‘adequate’ protection for individuals’ rights and freedoms for their personal data.

Adequacy decisions made prior to GDPR, remain in force unless there is a further Commission decision which decides otherwise. The Commission plans to review these decisions at least once every four years.

If it is covered by an adequacy decision, you may go ahead with the restricted transfer. Of course, you must still comply with the rest of the GDPR.

All EU Commission adequacy decisions to date also cover restricted transfers made from EEA states. The EEA Joint Committee will need to make a formal decision to adopt any future EU Commission adequacy decisions, for them to cover restricted transfers from EEA states.

1) What 'adequacy decisions' have there been?

As at July 2018 the Commission has made a full finding of adequacy about the following countries and territories:

Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

The Commission has made partial findings of adequacy about Canada and the USA.

- The adequacy finding for Canada only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. For more details please see the [Commission's FAQs](#) on the adequacy finding on the Canadian PIPEDA.
- The adequacy finding for the USA is only for personal data transfers covered by the EU-US Privacy Shield framework.

The Privacy Shield places requirements on US companies certified by the scheme to protect personal data and provides for redress mechanisms for individuals. US Government departments such as the Department of Commerce oversee certification under the scheme.

If you want to transfer personal data to a US organisation under the Privacy Shield, you need to:

- check on the [Privacy Shield list](#) to see whether the organisation has a current certification; and
- make sure the certification covers the type of data you want to transfer.

We are expecting an adequacy decision for Japan soon.

You can view an up to date list of the countries which have an adequacy finding on [the European Commission's data protection website](#). You should check back regularly for any changes.

2) What if there is no adequacy decision?

You should move on to the next section [Is the transfer covered by appropriate safeguards?](#)

Further Reading

 [Relevant provisions in the GDPR – see Article 45 and Recitals 103-107 and 169](#)

External link

In more detail - ICO guidance

[Using the privacy shield to transfer data to the US](#)

Other resources

See the [Privacy Shield website](#) for more information.

Is the restricted transfer covered by appropriate safeguards?

If there is no 'adequacy decision' about the country, territory or sector for your restricted transfer, you should then find out whether you can make the transfer subject to 'appropriate safeguards', which are listed in the GDPR.

These appropriate safeguards ensure that both you and the receiver of the transfer are legally required to protect individuals' rights and freedoms for their personal data.

If it is covered by an appropriate safeguards, you may go ahead with the restricted transfer. Of course, you must still comply with the rest of the GDPR.

Each appropriate safeguard is set out below:

1. A legally binding and enforceable instrument between public authorities or bodies

You can make a restricted transfer if you are a public authority or body and you are transferring to another public authority or body, and you have both signed a contract or another legal instrument which is legally binding and enforceable. This contract or instrument must include enforceable rights and effective remedies for individuals whose personal data is transferred.

This is not an appropriate safeguard if either you or the receiver are a private body or an individual.

If you are a public authority or body which does not have the power to enter into legally binding and enforceable arrangements, you may consider [an administrative arrangement which includes enforceable and effective individual rights](#).

Further Reading

 [Relevant provisions in the GDPR – see Article 46 and Recitals 108-109 and 114](#) 

External link

2. Binding corporate rules

You can make a restricted transfer if both you and the receiver have signed up to a group document called binding corporate rules (BCRs).

BCRs are an internal code of conduct operating within a multinational group, which applies to restricted transfers of personal data from the group's EEA entities to non-EEA group entities.

This may be a corporate group or a group of undertakings or enterprises engaged in a joint economic activity, such as franchises or joint ventures.

You must submit BCRs for approval to an EEA supervisory authority in an EEA country where one of the companies is based. Usually this is where the EEA head office is located, but it does not need to be. The criteria for choosing the lead authority for BCRs is laid down in the "Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR" (see "In more detail" below).

One or two other supervisory authorities will be involved in the review and approval of BCRs (depending on how many EEA countries you are making restricted transfers from). These will be supervisory authorities where other companies signing up to those BCRs are located.

The concept of using BCRs to provide adequate safeguards for making restricted transfers was developed by the Article 29 Working Party in a series of working documents. These form a 'toolkit' for organisations. The documents, including application forms and guidance have all been revised and updated in line with GDPR (see "In more detail" below).


In more detail - European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state and each EEA state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 adopted the following guidelines, which have been endorsed by the EDPB:

[Table of elements and principles for controller BCRs](#)  (WP256)

[Table of elements and principles for processor BCRs](#)  (WP257)

[Co-Operation Procedure for the approval of "Binding Corporate Rules"](#)  (WP263.01)

[Application Form BCR - C](#)  (WP264)

[Application Form BCR - P](#)  (WP265)

Further Reading

 [Relevant provisions in the GDPR – see Articles 46-47 and Recitals 108-110 and 114](#) 

External link

3. Standard data protection clauses adopted by the Commission

You can make a restricted transfer if you and the receiver have entered into a contract incorporating standard data protection clauses adopted by the Commission.

These are known as the 'standard contractual clauses' (sometimes as 'model clauses'). There are four sets which the Commission adopted under the Directive. They must be entered into by the data exporter (based in the EEA) and the data importer (outside the EEA).

The clauses contain contractual obligations on the data exporter and the data importer, and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the data importer and the data exporter.

There are two sets of standard contractual clauses for restricted transfers between a controller and controller, and two sets between a controller and processor. The earlier set of clauses between a controller and processor can no longer be used for new contracts, and are only valid for contracts entered into prior to 2010.

The Commission plans to update the existing standard contractual clauses for the GDPR. Until then, you can still enter into contracts which include the Directive-based standard contractual clauses. Please keep checking the websites of the ICO and the Commission for further information.

Existing contracts incorporating standard contractual clauses can continue to be used for restricted

transfers (even once the Commission has adopted GDPR standard contractual clauses).

If you are entering into a new contract, you must use the standard contractual clauses **in their entirety and without amendment**. You can include additional clauses on business related issues, provided that they do not contradict the standard contractual clauses. You can also add parties (i.e. additional data importers or exporters) provided they are also bound by the standard contractual clauses.

If you are making a restricted transfer from a controller to another controller, you can choose which set of clauses to use, depending on which best suits your business arrangements.

Example

A family books a holiday in Australia with a UK travel company. The UK travel company sends details of the booking to the Australian hotel.

Each company is a separate controller, as it is processing the personal data for its own purposes and making its own decisions.

The contract between the UK travel company and the hotel should use controller to controller standard contractual clauses.

If you are making a restricted transfer from a controller to a processor, you also need to comply with [the GDPR requirements about using processors](#).

In more detail

The Commission published the following standard contractual clauses:

[2001 controller to controller](#)

[2004 controller to controller](#)

[2010 controller to processor](#)

Further Reading

[Relevant provisions in the GDPR – see Article 46 and Recitals 108-109 and 114](#)

External link

4. Standard data protection clauses adopted by a supervisory authority and approved by the Commission.

You can make a restricted transfer from the UK if you enter into a contract incorporating standard data protection clauses adopted by the ICO.

However, neither the ICO nor any other EEA supervisory authority has yet adopted any standard data

protection clauses.

They are likely to be similar to those adopted by the Commission (above), but will be first adopted by the supervisory authority and then approved by the Commission.

We will add more details about using this option in due course.

Further Reading

 [Relevant provisions in the GDPR – see Article 46 and Recitals 108-109 and 114](#) 

External link

5. An approved code of conduct together with binding and enforceable commitments of the receiver outside the EEA

You can make a restricted transfer if the receiver has signed up to a code of conduct, which has been approved by a supervisory authority. The code of conduct must include appropriate safeguards to protect the rights of individuals whose personal data transferred, and which can be directly enforced.

The GDPR endorses the use of [approved codes of conduct](#) to demonstrate compliance with its requirements.

This option is newly introduced by the GDPR and no approved codes of conduct are yet in use. We will add more details about this option in due course.

Further Reading

 [Relevant provisions in the GDPR – see Article 46 and Recitals 108-109 and 114](#) 

External link

In more detail - European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state and each EEA state. It adopts guidelines for complying with the requirements of the GDPR.

The EDPB is producing guidance on codes of conduct, in general and in relation to restricted transfers, which will be published in due course.

6. Certification under an approved certification mechanism together with binding and enforceable commitments of the receiver outside the EEA

You can make a restricted transfer if the receiver has a certification, under a scheme approved by a supervisory authority. The certification scheme must include appropriate safeguards to protect the rights of individuals whose personal data transferred, and which can be directly enforced.

The GDPR also endorses the use of [approved certification mechanisms](#) to demonstrate compliance with its requirements.

This option is newly introduced by the GDPR and no approved certification schemes are yet in use. We will add more details about this option in due course.

Further Reading

 [Relevant provisions in the GDPR – see Article 46 and Recitals 108-109 and 114](#) 

External link

In more detail - European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state and each EEA state. It adopts guidelines for complying with the requirements of the GDPR.

The EDPB is producing guidance on certification schemes, in general and in relation to restricted transfers, which will be published in due course.

7. Contractual clauses authorised by a supervisory authority

You can make a restricted transfer if you and the receiver have entered into a bespoke contract governing a specific restricted transfer which has been individually authorised by the supervisory authority of the country from which the personal data is being exported. If you are making a restricted transfer from the UK, the ICO will have had to have approved the contract.

At present the ICO is not authorising any such bespoke contracts, until guidance has been produced by the EDPB.

8. Administrative arrangements between public authorities or bodies which include enforceable and effective rights for the individuals whose personal data is transferred, and which have been authorised by a supervisory authority

You can make a restricted transfer if:

- you are a public authority or body making a transfer to one or more public authorities or bodies;
- at least one of the public authorities or bodies does not have the power to use any of the other appropriate safeguards (set out above). For example, it cannot enter into a binding contract;
- you and the receiver have entered into an administrative arrangement, (usually a document) setting out appropriate safeguards regarding the personal data to be transferred and which provides for effective and enforceable rights by the individuals whose personal data is transferred; or
- the administrative arrangement has been individually authorised by the supervisory authority in the country (or countries) from which you are making the restricted transfer. If the restricted transfer is to be made from the UK, the ICO must approve it.

This is not an appropriate safeguard for restricted transfers between a public and private body.

This option is newly introduced by the GDPR and no approved administrative arrangements are yet in use. We will add more details about this option in due course.

In more detail - European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state and each EEA state. It adopts guidelines for complying with the requirements of the GDPR.

The EDPB is producing guidance on administrative arrangements, which will be published in due course.

Further Reading

 [Relevant provisions in the GDPR – see Article 46 and Recitals 108-109 and 114](#) 
External link

What if the restricted transfer is not covered by appropriate safeguards?

If the restricted transfer is not covered by appropriate safeguards, then you need to consider the next question: [Is the restricted transfer covered by an exception?](#)

Is the restricted transfer covered by an exception?

If you are making a restricted transfer that is not covered by an adequacy decision, nor an appropriate safeguard, then you can only make that transfer if it is covered by one of the 'exceptions' set out in Article 49 of the GDPR.

You should only use these as true 'exceptions' from the general rule that you should not make a restricted transfer unless it is covered by an adequacy decision or there are [appropriate safeguards](#) in place.

If it is covered by an exception, you may go ahead with the restricted transfer. Of course, you must still comply with the rest of the GDPR.

Each exception is set out below:

Exception 1. Has the individual given his or her explicit consent to the restricted transfer?

Please see the [section on consent](#) as to what is required for a valid explicit consent under the GDPR.

As a valid consent must be both specific and informed, you must provide the individual with precise details about the restricted transfer. You cannot obtain a valid consent for restricted transfers in general.

You should tell the individual:

- the identity of the receiver, or the categories of receiver;
- the country or countries to which the data is to be transferred;
- why you need to make a restricted transfer;
- the type of data;
- the individual's right to withdraw consent; and

- the possible risks involved in making a transfer to a country which does not provide adequate protection for personal data and without any other [appropriate safeguards](#) in place. For example, you might explain that there will be no local supervisory authority, and no (or only limited) individual data protection or privacy rights.

Given the high threshold for a valid consent, and that the consent must be capable of being withdrawn, this may mean that using consent is not a feasible solution.

Exception 2. Do you have a contract with the individual? Is the restricted transfer necessary for you to perform that contract?

Are you about to enter into a contract with the individual? Is the restricted transfer necessary for you to take steps requested by the individual in order to enter into that contract?

This exception explicitly states that it can only be used for **occasional** restricted transfers. This means that the restricted transfer may happen more than once but not regularly. If you are regularly making restricted transfers, you should be putting in place [an appropriate safeguard](#).

The transfer must also be **necessary**, which means that you cannot perform the core purpose of the contract or the core purpose of the steps needed to enter into the contract, without making the restricted transfer. It does not cover a transfer for you to use a cloud based IT system.

Example

A UK travel company offering bespoke travel arrangements may rely on this exception to send personal data to a hotel in Peru, provided that it does not regularly arrange for its customers to stay at that hotel. If it did, it should consider using an appropriate safeguard, such as the [the standard contractual clauses](#).

It is only necessary to send limited personal data for this purpose, such as the name of the guest, the room required and the length of stay.

Example of necessary steps being taken at the individual's request in order to enter into a contract: Before the package is confirmed (and the contract entered into), the individual wishes to reserve a room in the Peruvian hotel. The UK travel company has to send the Peruvian hotel the name of the customer in order to hold the room.

Public authorities cannot rely on this exception when exercising their public powers.

Exception 3. Do you have (or are you entering into) a contract with an individual which benefits another individual whose data is being transferred? Is that transfer necessary for you to either enter into that contract or perform that contract?

As set out in Exception 2, you may only use this exception for occasional transfers, and the transfer must be necessary for you to perform the core purposes of the contract or to enter into that contract.

You may rely on both Exceptions 2 and 3: Exception 2 for the individual entering into the contract and Exception 3 for other people benefiting from that contract, often family members.

Exceptions 2 and 3 are not identical. You cannot rely on Exception 3 for any restricted transfers needed for steps taken prior to entering in to the contract.

Public authorities cannot rely on this exception when exercising their public powers.

Example

Following the Exception 2 example, Exception 3 may apply if the customer is buying the travel package for themselves and their family. Once the customer has bought the package with the UK travel company, it may be necessary to send the names of the family members to Peruvian hotel in order to book the rooms.

Exception 4: You need to make the restricted transfer for important reasons of public interest.

There must be an EU or UK law which states or implies that this type of transfer is allowed for important reasons of public interest, which may be in the spirit of reciprocity for international co-operation. For example an international agreement or convention (which the UK or EU has signed) that recognises certain objectives and provides for international co-operation (such as the [2005 International Convention for the Suppression of Acts of Nuclear Terrorism](#)).

This can be relied upon by both public and private entities.

If a request is made by a non-EEA authority, requesting a restrictive transfer under this exception, and there is an international agreement such as a mutual assistance treaty (MLAT), you should consider referring the request to the existing MLAT or agreement.

You should not rely on this exception for systematic transfers. Instead, you should consider one of the [appropriate safeguards](#). You should only use it in specific situations, and each time you should satisfy yourself that the transfer is necessary for an important reason of public interest.

Exception 5: You need to make the restricted transfer to establish if you have a legal claim, to make a legal claim or to defend a legal claim.

This exception explicitly states that you can only use it for **occasional** transfers. This means that the transfer may happen more than once but not regularly. If you are regularly transferring personal data, you should put in place an [appropriate safeguard](#).

The transfer must be necessary, so there must be a close connection between the need for the transfer and the relevant legal claim.

The claim must have a basis in law, and a formal legally defined process, but it is not just judicial or administrative procedures. This means that you can interpret what is a legal claim quite widely, to cover, for example:

- all judicial legal claims, in civil law (including contract law) and criminal law. The court procedure does not need to have been started, and it covers out-of-court procedures. It covers formal pre-trial discovery procedures.
- administrative or regulatory procedures, such as to defend an investigation (or potential

investigation) in anti-trust law or financial services regulation, or to seek approval for a merger.

You cannot rely on this exception if there is only the mere possibility that a legal claim or other formal proceedings may be brought in the future.

Public authorities can rely on this exception, in relation to the exercise of their powers.

Exception 6: You need to make the restricted transfer to protect the vital interests of an individual. He or she must be physically or legally incapable of giving consent.

This applies in a medical emergency where the transfer is needed in order to give the medical care required. The imminent risk of serious harm to the individual must outweigh any data protection concerns.

You cannot rely on this exception to carry out general medical research.

If the individual is physically and legally capable of giving consent, then you cannot rely on this exception.

For detail as to what is considered a 'vital interest' under the GDPR, please see [the section on vital interests as a condition of processing special category data](#).

For detail as to what is 'consent' under the GDPR please see the [section on consent](#).

Exception 7: You are making the restricted transfer from a public register.

The register must be created under UK or EU law and must be open to either:

- the public in general; or
- any person who can demonstrate a legitimate interest.

For example, registers of companies, associations, criminal convictions, land registers or public vehicle registers. The whole of the register cannot be transferred, nor whole categories of personal data.

The transfer must comply with any general laws which apply to disclosures from the public register. If the register has been established at law and access is only given to those with a legitimate interest, part of that assessment must take into account the data protection rights of the individuals whose personal data is to be transferred. This may include consideration of the risk to that personal data by transferring it to a country with less protection.

This does not cover registers run by private companies, such as credit reference databases.

Exception 8: you are making a one-off restricted transfer and it is in your compelling legitimate interests.

If you cannot rely on any of the other exceptions, there is one final exception to consider. This exception should not be relied on lightly and never routinely as it is only for truly exceptional circumstances.

For this exception to apply to your restricted transfer:

1. there must be no adequacy decision which applies.
2. you are unable to use any of the other appropriate safeguards. You must give serious consideration to this, even if it would involve significant investment from you.
3. none of the other exceptions apply. Again, you must give serious consideration to the other

exceptions. It may be that you can obtain explicit consent with some effort or investment.

4. your transfer must not be repetitive – that is it may happen more than once but not regularly.
5. the personal data must only relate to a limited number of individuals. There is no absolute threshold for this. The number of individuals involved should be part of the balancing exercise you must undertake in para (g) below.
6. The transfer must be necessary for your compelling legitimate interests. Please see the section of the guide on [legitimate interests as a lawful basis for processing](#), but bearing mind that this exception requires a higher standard, as it must be a compelling legitimate interest. An example is a transfer of personal data to protect a company's IT systems from serious immediate harm.
7. On balance, your compelling legitimate interests outweigh the rights and freedoms of the individuals.
8. You have made a full assessment of the circumstances surrounding the transfer and provided suitable safeguards to protect the personal data. Suitable safeguards might be strict confidentiality agreements, a requirement for data to be deleted soon after transfer, technical controls to prevent the use of the data for other purposes, or sending pseudonymised or encrypted data. This must be recorded in full in your [documentation of your processing activities](#).
9. You have informed the ICO of the transfer. We will ask to see full details of all the steps you have taken as set out above.
10. You have informed the individual of the transfer and explained your compelling legitimate interest to them.

Further Reading

 [Relevant provisions in the GDPR – see Article 49 and Recitals 111-112](#) 

External link

In more detail - European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state and each EEA state. It adopts guidelines for complying with the requirements of the GDPR.

The EDPB adopted [Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679](#) 