



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

Data protection guidelines

International transfers of personal information

General advice on how to comply with the 8th data protection principle

This guidance provides practical advice to companies or other organisations who want to transfer personal information outside the European Economic Area (EEA). It is not a complete statement of the relevant law, this is provided in [‘The eighth data protection principle and international data transfers’](#) which is on our website.

This guidance only deals with the 8th data protection principle. It does not deal with other aspects of international transfers, for example, the security requirements of the 7th data protection principle. It also does not cover the other data protection principles you must comply with, particularly the 1st principle (which in most cases will require that individuals are informed about the transfer of their information to a third party outside the EEA).

The 8th principle

To comply with the 8th principle you must not transfer personal information to a country or territory outside the EEA unless there is an adequate level of protection for the information and for the rights of individuals.

Approaching the problem

We suggest you consider the following questions.

- Is it possible to fulfil your objectives without transferring personal information?
- Is there actually a transfer of personal information taking place?

- Is the destination country outside the EEA?
- Has the country been confirmed as 'adequate' by the European Commission?
- Are there other ways to achieve adequacy?
- Do any of the exemptions apply?

Is it possible to fulfil your objectives without transferring personal information?

Before making a transfer or otherwise processing personal information, you should consider whether it is possible to achieve your aims without actually processing personal information. For example, if personal information is anonymised so that it is not possible to identify individuals from it, then the data protection principles will not apply and you are free to transfer the information outside the EEA.

Is there a transfer?

A transfer involves sending information to a recipient in another country. This is not the same as transit through a country. The 8th principle will only apply if the information moves to, rather than simply passes through, a country outside the EEA.

For example, if personal information is transferred from country 'A' to country 'B' via a server in country 'C' and no access to or manipulation of the information happens in country 'C', then the transfer is only to country 'B'.

A transfer also takes place if the personal information you send is not currently subject to the Act, but will be after transfer.

For example, paper notes made about an identifiable individual, although not held on computer or as part of a relevant filing system in the UK, are sent by phone or fax to someone in another country where they will be entered on a computer or kept in a relevant filing system in that country.

Putting personal information on a website will often result in transfers to countries outside the UK. The transfers will take place when the website is accessed by someone outside the UK. If you load information onto a server based in the UK so that it can be

accessed through a website you should consider the potential for a transfer to take place and whether that would be fair for the individuals involved given the potential effect on them. If it is your intention that the information will be accessed outside the EEA, then this is a transfer. For more information on this, see the section on the Lindqvist case in [‘The eighth data protection principle and international data transfers’](#) which is on our website.

Is the destination country outside the European Economic Area (EEA)?

There are no restrictions on the transfer of personal information to other EEA countries. These are currently:

Austria	Estonia	Iceland	Luxembourg	Romania
Belgium	Finland	Ireland	Malta	Slovakia
Bulgaria	France	Italy	Netherlands	Slovenia
Czech Republic	Germany	Latvia	Norway	Spain
Cyprus	Greece	Liechtenstein	Poland	Sweden
Denmark	Hungary	Lithuania	Portugal	

Has the country been confirmed as ‘adequate’ by the European Commission?

The European Commission (EC) can decide if a country has an adequate level of protection for personal information. Currently, the following countries are considered adequate.

Argentina	Canada	Guernsey	Isle of Man	Switzerland
Jersey				

For an up-to-date list of countries considered to be adequate, please see the European Commission’s data protection website at:

www.europa.eu.int/comm/justice_home/fsj/privacy/thirdcountries/index_en.htm.

The USA

In the USA there are laws that apply to specific industries which provide some protection for personal information, but there is no general data protection law. The Privacy Act 1974 establishes certain controls over how the executive branch agencies of the federal government gather, maintain, and disseminate personal information. The Privacy Act can also be used to obtain access to information, but it applies only to records the federal government keeps on US citizens and lawfully admitted resident aliens.

However, the European Commission considers the 'Safe Harbor' scheme to provide an adequate level of protection. When a US company signs up to the Safe Harbor arrangement, they agree to follow seven principles of information handling and that they can be held responsible for keeping to those principles by the Federal Trade Commission or other oversight schemes. You can find a list of the US companies signed up to the Safe Harbor arrangement on the US Department of Commerce website at http://www.export.gov/safeharbor/doc_safeharbor_index.asp.

In July 2007, the EU and the USA signed an agreement to legitimise and regulate the transfer of passenger name record information (PNR) from EU airlines to the US Department of Homeland Security (DHS).

Are there other ways to achieve adequacy?

Even if the European Commission has not decided that the law in a country is adequate, you can still transfer personal information if you are satisfied that the particular circumstances of the transfer ensure an adequate level of protection. The Data Protection Act 1998 (the Act) sets out the factors you should take into account to make this decision. These relate to:

- the nature of the information being transferred;
- how the information will be used and for how long; and
- the laws and practices of the country you are transferring the information to.

This means you carrying out some form of risk assessment. You must decide whether, in all the circumstances of the transfer, there is enough protection for individuals. This is known as an assessment of adequacy. To assess adequacy you should look at:

- the extent to which the country has adopted data protection standards in its law;
- whether there is a way to make sure the standards are achieved in practice; and
- whether there is an effective procedure for individuals to enforce their rights or get compensation if things go wrong.

We realise that it may be impractical for you to carry out a detailed analysis of adequacy involving the legal situation in a non-EEA country. This analysis might be more appropriate for a business that regularly transfers large volumes of information to a particular country, rather than a company that might only occasionally transfer information to any of a wide range of countries. For this reason, this guidance does not give detailed advice on how to carry out an adequacy test, this is provided in sections 2.3 to 2.6 of 'The eighth data protection principle and international data transfers'.

There are some cases where you might reasonably decide that there is adequacy without carrying out a detailed test. One of these is where you transfer information to a processor acting on your instructions under contract. This is likely to be a common situation. You are still legally responsible for making sure the information is processed in line with the principles. In particular information cannot be transferred without there being a contract in place requiring the processor to have appropriate security and act only on your instruction. Therefore individuals' information should continue to be protected to the same standard as in the UK and they will have the same rights which they can exercise in the UK. When selecting a processor you need to satisfy yourself that it is reliable and has appropriate security in place.

However, if the transfer is to a processor in an unstable country and the nature of the information means that it is at particular risk, then it is unlikely that there will be adequacy. For more information see section 5 of 'The eighth data protection principle and international data transfers' and the good practice note on outsourcing on our website.

There might also be other cases where the nature of the information and the circumstances of the transfer, along with your knowledge of the country of transfer and the particular company you are transferring to, mean it is reasonable to decide there is adequacy without a detailed analysis. Some examples are discussed below.

A university wishes to transfer the academic biographies of its lecturers and research staff to other universities and potential students outside the EEA. Nothing of a private nature is included. This is a well-known practice in the university. The personal information, such as the qualifications and publications of the staff, is already publicly available and any member of staff who has particular reason to have their information withheld, for example, concerns about their safety, can have their information withheld. It is difficult to see a problem with adequacy as the potential for staff to object has been addressed and there is little further risk of misuse.

Company A in the UK sends its customer list to company B outside the EEA so that company B, acting as a processor, can send a mailing to company A's customers. It is likely that adequate protection exists if:

- the information transferred is only names and addresses;
- there is nothing particularly sensitive about company A's line of business;
- the names and addresses are for one-time use and must be returned or destroyed within a short timescale;
- company A knows company B is reliable; and
- there is a contract between them governing how the information will be used.

An employee travels outside the EEA with a laptop containing personal information connected with their employment. Their employer in the UK is still the data controller. As long as the information stays with the employee on the laptop, and the employer has an effective procedure to deal with security and the other risks of using laptops (including the extra risks of international travel), it is reasonable to decide that adequate protection exists.

A multinational company transfers a list of internal telephone extensions to its own overseas subsidiaries. The nature of the information means that it is unlikely that the individuals identified would suffer significant damage in the unlikely event that it was obtained by an unauthorised source. It is reasonable to decide that adequate protection exists.

From these examples we can see that you can, at least in part, decide whether there is adequacy. You might limit the types of information you transfer, the types of organisation you transfer to, or insist, through a contract or otherwise, that the destination company meet certain conditions.

Contracts

There are several different types of contract which you can use to transfer personal information outside the EEA. In practice, the main types of contracts are:

- contracts based on the standard contractual clauses approved by the European Commission (EC model clauses); and
- other contracts you draw up to bring protection up to an adequate level.

EC model clauses

The EC has approved three sets of standard contractual clauses (known as model clauses) as providing adequate protection to transfer individuals' personal information, so if you use these clauses you will not have to make your own assessment of adequacy. Two sets of model clauses relate to transferring personal information from one company to another company who will use it for its own purposes and you can choose either depending upon which set suits your business arrangements better. The other set is for transferring personal information to a processor acting under your instructions. The model clauses are attached as an annex to the EC decisions of adequacy which approve their use, and you can find them on their data protection website at:

www.europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm.

If you are relying on the EC's approval, you cannot change the clauses in any way. For more information, see section 3.2 of 'The eighth data protection principle and international data transfers'.

Other contracts

You can use other contracts to help make sure there is adequacy in a particular transfer or set of transfers. **We are not able to give detailed advice on or approve contracts other than in exceptional circumstances.** You can use these contracts to plug gaps where you have decided that, were it not for a particular weakness, adequacy would exist. For example, you may want to include a contract clause to require the company receiving the information to return it to you if your relationship comes to an end or if they go out of business.

You do not have to have a separate contract for data protection. You can include the terms to achieve adequacy into any general contract that covers your relationship with the other company.

You can also use contracts where you are not in a position to judge if adequacy exists. Rather than plugging known gaps in adequacy, the contract should be comprehensive to enable you to satisfy yourself that adequacy exists, without you needing to analyse the circumstances of the transfer. This kind of contract is likely to be very similar to a standard contract using the EC model clauses which you can use to develop your own terms.

If you use contracts other than the model clauses, you take the risk that there could be a future challenge as to whether the contract did in fact cover adequacy. You must record how you make sure you comply with the Act, and be able to justify your actions if you are asked to. This is in line with our general approach to compliance with the Act.

Authorised arrangements

We do not expect to authorise one-off arrangements between you and companies in other countries other than in exceptional circumstances. Before we authorise any one-off arrangements, we would want to be satisfied that there was no other reasonable way for you to comply with the 8th principle and that you could not rely on any of the exceptions.

Where we authorise any arrangement, we must tell the EC and other data protection authorities in Europe. If you want us to authorise a one-off arrangement, we advise you to consult us before developing your proposals.

Binding corporate rules

Another option (which only applies to multinational organisations transferring personal information outside the EEA, but within their group of companies) is to adopt binding codes of corporate conduct (known as binding corporate rules or BCR). These rules may include intra-group agreements, policies or procedures, and special arrangements among the group of companies that provide the necessary protection. To use BCR to transfer personal information freely within the group, they must be approved by all the relevant EU data protection authorities who will co-operate with one another when making authorisations and to make sure that the rules are complied with.

It is also possible to use internal codes of conduct, similar in substance to BCR, to transfer information from the UK without an authorisation where you have conducted a risk assessment and are satisfied that the codes provide the level of safeguards required by the 8th principle. Where you do not have an authorisation you take the risk that there could be a future challenge as to whether the codes do in fact provide adequacy. You must record how you make sure you comply with the Act, and be able to justify your actions if you are asked to. This is in line with our general approach to compliance with the Act.

For more information on BCR see section 3.3 of 'The eighth data protection principle and international data transfers' and the [international transfers page](#) on our website (www.ico.gov.uk).

Do any of the exemptions apply?

There are several exemptions from the 8th principle where you can transfer personal information even if there is no adequate protection. We consider that an individual's personal information is better protected if you take steps to make sure there is adequacy rather than simply relying on an exemption. However, the exemptions are available to you under law and may in some circumstances provide a simple solution that only

results in a minimal loss of protection for the individual. For a detailed analysis of the exemptions see section 4 of 'The eighth data protection principle and international data transfers'.

- **Consent**

You can transfer information if you have the individual's consent, which should be explicit, given freely and can subsequently be withdrawn by the individual. Consent is sometimes made a condition of providing a non-essential service but it is unlikely to be valid if the individual has no choice but to give their consent.

For example, if you ask an employee to agree to the international transfer of personal information, their consent will not be valid if the penalty for not agreeing is dismissal.

The individual must know and have understood what they are agreeing to. You should specify the reasons for the transfer and as far as possible the countries involved. If you are aware of any particular risks involved in the transfer, you should tell the individual. Although you need to consider all the circumstances of a particular case, it is possible to give some general examples.

'By signing below you accept that we can transfer any of the information we keep about you to any country when a business need arises.'	Any consent given is unlikely to be valid. This term may also be unfair in a contract with a consumer.
'By signing below you accept that we will pass details of your mortgage application to company A in Singapore who we have chosen to arrange mortgages on our behalf. You should be aware that Singapore does not have a data protection law.'	Any consent given is likely to be valid.
'By signing below you agree that we may pass relevant personnel records to our subsidiary companies in any country we	Any consent given is likely to be valid in the case of an employee of a multinational group who accepts a job

transfer you to. We will continue to handle your records in line with our code of good practice, although you might no longer have rights under data protection law.'	involving international postings, and where the multinational has a group-wide data protection code.
'By signing below you agree that we will pass information about you and your policy to other insurance companies with which we reinsure our business. These companies may be in countries outside the UK that do not have laws to protect your information. You can get details of the companies and countries involved in your case if you ask us.'	Any consent given is likely to be valid where it is not practical to list all the re-insurers and the countries they are in because the list is too long, because it changes regularly or because different re-insurers from the list are used in different circumstances.

You can get more advice on consent in chapter 3 of 'The eighth data protection principle and international data transfers'. You should be aware that it is the Information Commissioner's view that consent is unlikely to provide an adequate long-term solution to repeated transfers or ones that arise from a structural reorganisation.

- **Contract performance**

You can transfer information where it is **necessary** for carrying out certain types of contract or if the transfer is **necessary** to set up the contract.

- A contract between the company and the individual:
 - the transfer is necessary to carry out the contract; **or**
 - the transfer is a necessary part of the steps the individual has asked you to take before a contract is made between you.
- A contract between the company and someone other than the individual:
 - the individual requests the contract or it is in their interests; **and**
 - the transfer is necessary to conclude the contract; **or**
 - the transfer is necessary to carry out such a contract.

In this context contracts are not restricted to goods and services, they can include employment contracts. Deciding whether a transfer is necessary to carry out a contract depends on the nature of the goods or services provided under the contract rather than how your business is organised. A transfer is not necessary if the only reason you need to make it is because of the way you have chosen to structure your business. For example:

- If a customer books a hotel in the USA through a UK travel agent, the UK travel agent will need to transfer the booking details to the USA to fulfil its contract with the customer.
- If the customer of a UK credit-card holder uses their card in Japan, it may be necessary for the card issuer to transfer some personal information to Japan to validate the card or reimburse the seller (or both).
- A UK-based internet trader might sell furniture on-line. It makes it clear to customers that it is a retailer, not a manufacturer. Goods are delivered direct to the customer from the manufacturer. If a customer orders goods that are manufactured in the Ukraine, the trader needs to transfer a delivery name and address to the Ukraine to carry out the contract.
- If the same UK-based retailer has its accounts department outside the UK, transferring personal information to the accounts department is not necessary to carry out a contract. It may be necessary because of the decision to relocate the accounts department, but the contract could be carried out just as well if the accounts department was in the UK. In this case you will need to establish a different basis for the transfer.

- **Substantial public interest**

You can transfer information where it is **necessary** for reasons of substantial public interest. This is a high threshold to meet and it is most likely to be in areas such as preventing and detecting crime, national security and collecting tax. Companies intending to rely on this exemption should look at each case individually. The public

interest must be that of the UK and not the third country to which the information is transferred.

- **Vital interests**

You can transfer information where it is necessary to protect the vital interests of the individual. This relates to matters of 'life and death'.

For example: A local health authority could transfer relevant medical records from the UK to another country where an individual had had a heart attack and their medical history was necessary to decide on appropriate treatment.

- **Public registers**

You can transfer part of the personal information on a public register as long as the person you transfer to complies with any restrictions on access to or use of the information in the register.

For example: The General Medical Council can transfer extracts from its register of medical practitioners to respond to enquiries from outside the UK, but it is not allowed to transfer the complete register under this exemption. If the GMC puts conditions on inspecting the register in the UK, the person the extract is transferred to and anyone they then pass it on to must comply with these restrictions.

- **Legal claims**

You can transfer information where it is necessary:

- in connection with any legal proceedings (including future proceedings not yet underway);
- to get legal advice; **or**
- to establish, exercise or defend legal rights.

For example: A US parent company is sued by an employee of the UK subsidiary and the transfer of relevant employee to the US parent is required for the defence.

The legal proceedings do not have to involve you or the individual and the legal rights do not have to be those of you or the individual. Although this exemption could potentially apply widely, transfers are unlikely to fall under this category if they are not in connection with legal proceedings or to get legal advice.

Legal compulsion from outside the UK

If you are required to transfer personal information to a country outside the UK by the law of that country, there is no blanket exemption allowing the transfer to take place. The transfer might be necessary for reasons of public interest or in connection with legal proceedings, but this will not always be the case. You will have to make a decision based on the circumstances of the particular case and the nature of the legal request.

For example: Under the Sarbanes-Oxley Act 2002, accountancy firms operating in the USA must provide information to the Security and Exchanges Commission about any convictions of staff that are working on the accounts of US firms. The transfer of this information by UK firms will not be exempt from the 8th principle and they must find a way to legally transfer the information. One way would be to get the relevant individual's consent.