THE OFFICE OF THE
DATA PROTECTION
COMMISSIONER

Guidance on International Transfers / Eighth Principle

This guidance document outlines the considerations for transferring personal data from the Bailiwick of Guernsey to other jurisdictions.

This guidance relates to the Data Protection (Bailiwick of Guernsey) Law, 2001 ("the Law").

Table of Contents

Introduction

The Eighth Data Protection Principle prohibits the transfer of personal information to countries or territories outside the Bailiwick of Guernsey.

A transfer can only be made where there is adequate protection for the rights and freedoms of individuals in relation to the processing of information about them. This is intended to ensure that data protection rules cannot be circumvented by transferring personal information to a place where it will benefit from no legal protection and where individuals will have no rights in respect the way that information is used.

Transfers can still take place to countries which do not have equivalent data protection legislation where adequacy is ensured by other means in the particular circumstances of the transfer.

Scope

This advice is intended to provide practical guidance to data controllers who want to transfer personal data outside the Bailiwick of Guernsey ("the Bailiwick").

This advice only addresses compliance with the Eighth Data Protection Principle (8th Principle). It does not deal with other compliance issues that international transfers might give rise to. For example, compliance with the Seventh Data Protection Principle requires that the means of transfer incorporates appropriate security measures; if sensitive data are transferred there will need to be explicit consent or an alternative basis under Schedule 3 for the processing involved; requirements for notification (formerly registration) relating to international transfers will need to be met.

The Eighth Principle

The 8th Data Protection Principle requires that:-

> *"Personal data shall not be transferred to a country or territory outside the Bailiwick unless that country or territory ensures an*

adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".

There are some exceptions to the Principle whereby personal data can be transferred to a country that might not ensure an adequate level of protection.

Approaching the problem

Alternative approaches are possible but it is suggested data controllers wishing to transfer personal data consider the following questions:-

- Is there actually a transfer of personal data taking place?
- Is the destination country within the European Economic Area ("the EEA")?
- Has the country been designated as "adequate"?
- Are there alternative grounds for concluding it is nevertheless "adequate"?
- Does one or more of the exceptions apply?
- Is there an alternative basis for the transfer?

Is there a transfer?

Transfer is not the same as transit. The 8th Principle only comes into play if data move to rather than simply pass through a country outside the Bailiwick. If personal data pass through country 'B' on the way from the Bailiwick to country 'A', there is only likely to be a transfer to country 'B' if some substantive processing operation takes place en route. This would be the case if, for example, the data were accessed, combined with other data or altered.

A transfer takes place not only if the information transferred is held as personal data in the Bailiwick but also if it is intended that it will be held as personal data after transfer.

For example, the requirements of the 8th Principle apply if notes made about an identifiable individual, although not held on computer or as part of a relevant filing system in the Bailiwick, are telephoned or faxed to a colleague in another country with the intention that they will be entered on a computer or kept in a relevant filing system in that country.

Putting personal data on a web site will almost certainly involve transfers to countries outside the Bailiwick. The transfers are to any countries from which the web site is accessed.

Is the destination country within the European Economic Area ("the EEA")?

Providing you are satisfied that you have complied with the other provisions (and in particular the principles) of the Law, there are no additional restrictions on the transfer of personal data to EEA countries.

The European Economic Area comprises the following states :-

EU Countries				
	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	United Kingdom
Plus	Iceland	Liechtenstein	Norway	

States within the EEA are required to implement data protection legislation to meet the standard outlined in Directive 95/46/EC. As the Directive is the framework against which adequacy for non-EEA countries is assessed, such legislation can be considered to provide the necessary protection.

It should be remembered that the Channel Islands and the Isle of Man are not part of the EEA.

Has the country been designated as "adequate"?

Jurisdictions outside of the EEA can apply to have their data protection legislation designated as adequate by the European Commission. This adequacy designation is recognised by the Commissioner, thus enabling data transfers to meet the requirement of the 8th Principle.

At the date of publication the following have been designated as adequate:

Andorra	Argentina	Canada	Faeroe Islands	Guernsey
Isle of Man	Israel	Jersey	New Zealand	Switzerland
Uruguay				

Such a designation could be subject to restrictions. For example, a country could be designated as adequate only for transfers that do not include sensitive personal data.

Much attention is focused on the USA. Although there are some sector specific requirements, the USA has no general data protection law and appears unlikely to adopt one in the foreseeable future.

Following the judgement of the European Union Court of Justice on 6 October 2015 (Schrems v Data Protection Commissioner Case C362/14), the "Safe Harbour" arrangements, previously approved for adequacy purposes, have been suspended. In their place is the new EU-US Privacy Shield designed to provide greater protection for transfers to the USA.

The USA Transfer of Passenger Name Record (PNR) Data arrangements in place have also deemed adequate.

Are there alternative grounds for adequacy?

Even if a country has not been designated as adequate by the European Commission, a data controller can nevertheless come to its own conclusion that the country provides an adequate level of protection for a particular transfer or set of transfers.

The Law indicates the sort of factors the data controller should take into account in reaching such a decision. These relate to the nature of the data being transferred, how they will be used and the laws and practices of the country to which they are being transferred. It implies some form of risk assessment.

The data controller must decide whether, in all the circumstances of the case, there is sufficient protection for individuals. In assessing adequacy a data controller should look not just at the extent to which data protection standards have been adopted but also at whether there is a means of ensuring the standards are achieved in practice and whether there is an effective mechanism for individuals to enforce their rights or obtain redress if things go wrong.

It is recognised that a detailed analysis of adequacy in a non-EEA country will very often be impractical for a Bailiwick data controller. Such an analysis might be appropriate for a business that routinely transfers large volumes of data to a particular country. It is unlikely to be carried out by a data controller that might only occasionally transfer data to any of a wide range of countries. For this reason, this advice does not give detailed guidance on how to carry out an adequacy test.

There are some cases where a data controller might reasonably conclude that adequacy exists without carrying out a detailed adequacy test. The first of these is where data are transferred for processing under the data controller's instructions to a processor outside the Bailiwick. This is likely to be a common situation and an example is outlined below.

Company A in the Bailiwick sends its customer list to company B outside the Bailiwick 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.

Where personal data is transferred to a data processor the Bailiwick data controller remains in control of the data even though the data have left the Bailiwick to be processed elsewhere.

Here the 7th Principle requires the data controller to have a contract with the processor committing the processor to adopt proper security measures and act only on instructions from the controller. Such a contract should be sufficient to deliver adequacy unless there is a particular reason to suppose it does not, for example the data are sensitive and the transfer is to an unstable country where the data are clearly at risk regardless of any contract that is in place.

There might also be other cases where the nature of the data and the circumstances of the transfer coupled with the data controller's knowledge of the country of transfer and the particular recipient mean it is reasonable to conclude there is adequacy without the need for a detailed analysis. Some examples are discussed below:-

1. The sporting achievements of well-known athletes are gathered from published material in the UK and put on a web site. It is difficult to see that there could be a problem with adequacy. The personal data are already in the public domain, there is no obvious reason why a data subject might object to their transfer and there is little if any scope for misuse.

2. An employee travels abroad with a lap-top containing personal data connected with his/her employment. His/her employer in the Bailiwick remains the data controller. Provided the data remain in the possession of the employee and the employer has an effective procedure which addresses security and other risks posed by the use of lap-tops including the additional risks posed by international travel, a conclusion that there is adequate protection is likely to be reasonable.

3. A Bailiwick based bank has a branch in India which collects personal data on local customers. The data are transferred to the Bailiwick where they are processed and then transferred from the Bailiwick back to India. The customers' expectations will be that their data are treated in accordance with Indian law. Given the source of the data and that the Bank has no reason to suppose the data will be misused after transfer, a conclusion of adequacy is reasonable.

From these examples, it can be seen that concluding whether or not there is adequacy can, at least partly, be in the hands of the Bailiwick data controller. The data controller might limit the types of data transferred, the types of organisation they are transferred to or insist, whether through a contract or otherwise, on the recipient meeting certain conditions.

Do exceptions apply?

There are several exceptions whereby data controllers can transfer personal data even if no adequate protection exists. Although the Commissioner considers that in many cases data subjects are better protected if the data controller takes steps to ensure adequacy rather than simply relying on an exception, she recognises that data controllers are entitled to make use of the exceptions in the Law, that they will often provide a simple solution for the data controller and that the loss of protection for the individual might in practice be minimal.

Consent

Transfers can be made with the consent of the data subject. Consent should be freely given. It can be made a condition for the provision of a non-essential service but consent is unlikely to be valid if the data subject has no real choice but to give his/her consent. For example, if an existing employee is required to agree to the international transfer of personal data any consent given is unlikely to be valid if the penalty for not agreeing is dismissal.

Consent should also be specific and informed. The data subject must know and have understood what he/she is agreeing to. The reasons

for the transfer and as far as possible the countries involved should be specified. If the data controller is aware of any particular risks involved in the transfer it should bring these to the data subject's attention. Although all the circumstances of a particular case would need to be considered, 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?".

Unlikely to produce valid consent as it is not clear to the data subject what will be happening with their personal data. There is no way for the data subject to adequately assess any risk to their personal data.

"By signing below you accept that we may pass details of your mortgage application to XYZ Ltd 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".

Likely to produce valid consent as it is clear what will be happening to the data subject's personal data and why. The data subject has sufficient information to assess any risk to their personal data.

"By signing below you agree that we may pass relevant personnel records to our subsidiary companies in any country to which you are transferred. Your records will continue to be handled in accordance with our code of good practice although you might no longer have rights under data protection law".

Likely to produce valid consent in the case of an employee of a multinational group who accepts a job involving international postings and where the multinational has a group wide data protection code.

"By signing below you agree that we may pass information about you and your policy to other insurance companies with which we reinsure our business. These companies may be located in countries outside the UK that do not have laws to protect your information. Details of the companies and countries involved in your case will be provided on request".

Likely to be acceptable where it is not practicable to list all the reinsurers and the countries in which they are located because the list is too long, because it changes regularly or because different reinsurers from the list are used in different cases.

Contract Performance

Transfers can be made where certain types of contracts are in place or contemplated:

- a contract between the data controller and the data subject
  - the transfer is necessary for performance of the contract or
  - the transfer is a necessary part of pre-contractual steps taken by the data controller at the request of the data subject.

- a contract between the data controller and someone other than the data subject
  - the contract is entered into at the data subject's request or in his/her interests and
  - the transfer is necessary for performance of the contract or
  - the transfer is necessary for conclusion of the contract.

In this context, contracts are not restricted to goods and services. These provisions will, for example, be relevant in the case of employment contracts. The Commissioner takes the view that the determination of whether a transfer is "necessary" for the performance of a contract depends on the nature of the goods, services etc. provided under the contract rather than the business structure of the data controller. A transfer is not "necessary" if the only reason it is needed is because of the way a data controller has chosen to structure its business. For example:

Example	Necessary?
A customer books a hotel in the USA through a Bailiwick travel agent. The travel agent wants to transfer the booking details to the hotel in the USA to ensure that a room is available for the customer.	☑
A Bailiwick resident uses their credit card in Japan. The card issuer wants to transfer some personal data to Japan to validate the card.	☑
A Bailiwick based internet trader sells furniture on-line. It makes it clear to customers that it is a retailer, not a manufacturer and that goods are delivered directly from the manufacturer. A customer orders goods via the website from a manufacturer in Russia. The trader wants to transfer the order details and delivery name and address to the Russian manufacturer.	☑
The same Bailiwick retailer has located is accounts department out of the Islands and wants to transfer the personal details of the buyer to that department. The decision to structure the company this way is organisational and not due to any specific need related to the completion of the contract with the purchaser.	☒

Substantial Public Interest

Transfers can be made where they are necessary for reasons of substantial public interest. This is most likely to be in areas such as crime prevention and detection, national security and tax collection. The Commissioner advises data controllers intending to rely on this exception to adopt a similar case by case test to that required by many of the exemptions in the Law in particular Section 29 (the crime and taxation exemption).

A transfer of any personal data should only take place to the extent that there would be likely to be substantial prejudice to the public interest if the transfer of those personal data did not take place.

Legal Claims

Transfers can be made where they are necessary:

- in connection with any legal proceedings (including prospective proceedings) or
- for obtaining legal advice or
- otherwise for establishing, exercising or defending legal rights.

It is clear that the legal proceedings do not necessarily have to involve the data controller or the data subject and that the legal rights do not have to be those of either the data controller or the data subject. Although the application of this exception is potentially quite wide, it is not immediately obvious where transfers might be necessary for "establishing, exercising or defending legal rights" if they are not in connection with legal proceedings or for obtaining legal advice.

Vital Interests

Transfers can be made where they are necessary in order to protect the vital interests of the data subject. This relates largely to matters of "life and death". For example, it would cover the transfer of relevant medical records from Guernsey to another country where an individual had been taken seriously ill or involved in a serious accident.

Public Registers

Transfers can be made of part of the personal data on a public register provided any restrictions on access to or use of the information in the register is complied with by the person to whom the information is transferred. This appears to allow, for example, the General Medical Council to transfer extracts from its register of

medical practitioners to enable it to respond to enquiries from outside the UK but would not allow it to transfer the complete register. If there are conditions the GMC imposes on inspection of the register in the UK, those must be honoured by the person the extract is transferred to and anyone it is subsequently passed onto.

Legal Compulsion

It should be noted that there is no exception for legal compulsion. If a data controller in the Bailiwick is required by the law of another country to transfer personal data to that country there is no blanket exemption allowing the transfer to take place. It might of course be that the transfer is necessary for reasons of substantial public interest or is necessary in connection with legal proceedings but this will not necessarily be so. A judgement will have to be made based on the circumstances of the particular case and nature of the legal requirement.

Are there other alternatives?

There are several different types of contract between a data controller in the Bailiwick and a recipient of personal data in another country which can be used to facilitate a transfer. In some cases the contract is comprehensive and avoids the need for the data controller to make its own assessment as to whether the circumstances of a particular transfer or set of transfers ensure adequate protection.

In other cases the contract might be less comprehensive and is used to bring what the data controller has assessed to be a not wholly adequate level of protection provided by the circumstances of a transfer up to an adequate level. The main types of contracts are:-

- Set of rules adopted by a global company to provide legally binding protection for personal data transferred within that global company (Binding Corporate Rules)
- Contracts based on standard terms approved by the European Commission (EC standard contracts).
- Contracts based on standard terms approved by the UK Information Commissioner (UK standard contracts).

- Contracts drawn up by the data controller to bring protection up to an adequate level (non-standard contracts).
- One-off arrangements authorised by the UK Information Commissioner as ensuring adequate safeguards (authorised arrangements).

It should be noted that the final category is not restricted to contracts. The Commissioner has the power to authorise arrangements that are not contractually based.

Binding Corporate Rules

Binding Corporate Rules are designed to allow multinational companies to transfer personal data to parts of their business outside of the EEA in compliance with the 8th principle. The process involves the provision of submissions outlining data protection compliance within the group of companies to EEA data protection authorities who, if satisfied that adequate protection is given, issue an authorisation to transfer personal data. This is an intra-group arrangement and does not apply to transfers outside the organisation.

Whilst the Commissioner is not currently part of the process of approving BCR submissions, the existence of valid and complaint BCR arrangements is deemed adequate for transfers from Bailiwick entities to overseas entities in the same organisation.

EC Standard Contracts

Standard terms that have been approved by the EC, are published on the European Commission's web site (www.europa.eu.int).

UK Standard Contracts

Similarly the Information Commissioner can approve standard terms if satisfied that they will provide adequate safeguards for the rights and freedoms of individuals. Standard terms relating to the UK are

published on the UK Information Commissioner's website www.informationcommissioner.gov.uk.

Non-Standard Contracts

Contracts can be used as one of the means by which a data controller ensures there is adequacy associated with a particular transfer or set of transfers. It is not expected that such contracts will be submitted to the Commissioner for approval. Indeed, the Commissioner is not in a position to give detailed advice on or approval to non-standard contracts other than in exceptional circumstances.

These non-standard contracts may be used to plug gaps where the Bailiwick data controller has concluded that were it not for a particular weakness, which can be addressed by contract terms, adequacy would exist.

An example might be a contract clause that requires the recipient to return all personal data to the Bailiwick data controller in the event of the relationship between the recipient and the Bailiwick data controller coming to an end or the recipient going out of business.

There is no reason why a non-standard contract has to stand alone. The required effect can be achieved by incorporation of appropriate terms in the general contract covering the relationship between the Bailiwick data controller and the recipient. It should be remembered that if the recipient is acting as a processor, either wholly or in part, for the Bailiwick data controller, the 7th Principle requires that there must, in any case, be written contract terms relating to security.

Non-standard contracts can also be used where the Bailiwick data controller is not in a position to judge whether adequacy exists. Rather than plugging known gaps in adequacy, the contract is comprehensive and thereby ensures adequacy, without the data controller needing to consider whether adequacy exists in any case.

Such contracts can be developed by individual data controllers. It is beyond the scope of this guide to give advice on the terms that should be included. Such a contract is likely to be very similar to a

standard contract using terms approved by the EC (see para. 9.2) or the UK Information Commissioner.

Indeed there is no reason why standard terms, including those developed by the ICC and the CBI cannot be used in developing a non-standard contract. The difference here is that the decision on whether the standard terms provide adequate protection rests with the data controller rather than with the European Commission or the UK Information Commissioner.

Although standard terms used to construct non-standard contracts do not have to be approved by either the EC or the Commissioner, the Commissioner takes the view that it is proper for data controllers to use them in this way. The data controller takes a risk that there could be a subsequent challenge as to whether the contract used did in fact ensure adequacy. This is consistent with the approach to compliance, generally adopted throughout the Law which is that there is no system of prior approval by the Commissioner. Rather it is for the data controller to determine how it ensures compliance with the Law, and to be able to defend it actions should it be called on to do so subsequently.

Authorised Arrangements

For the above reasons the Commissioner does not envisage that one-off arrangements between data controllers in the Bailiwick and recipients in other countries will be authorised other than in exceptional circumstances. Before authorising any one-off arrangements, the Commissioner would want to be satisfied that there was no other reasonable way for the data controller to ensure adequacy and that the data controller could not rely on any of the exceptions.

It is difficult to see why one-off arrangements should be authorised where the Bailiwick data controller and the recipient are separate legal persons and can enter into contractual arrangements.

They can do this even if they are members of the same group of companies. There is a difficulty where the Bailiwick data controller and the recipient are the same legal person. Although contractual

solutions are not possible there may be other ways in which adequacy can be ensured, for example by the adoption of company-wide standards which a data subject can enforce against the Bailiwick company even if the breach occurs elsewhere.

Again, the Commissioner would want to be satisfied that all such possibilities had been considered before an authorisation was given. For this reason, obtaining an authorisation is unlikely to be either a quick or simple process. In the event of any authorisation being given, the Commissioner is under a duty to inform the European Commission and other Data Protection authorities. Data controllers intending to seek the Commissioner's authorisation for one-off arrangements are advised to consult her office before developing their proposals.

Contact the Commissioner

Enquiries and Publication Requests

Guernsey

Office of the Data Protection Commissioner
Guernsey Information Centre
North Esplanade
St Peter Port
Guernsey
GY1 2LQ

T: +44 (0)1481 742074
W: www.dataci.org
Email: enquiries@dataci.org