Information Commissioner's Office

Data Protection Act 1998

The eighth data protection principle and international data transfers

The Information Commissioner's recommended approach to assessing adequacy including consideration of the issue of contractual solutions, binding corporate rules and Safe Harbor.

Reproduction of this material is permitted on the basis that the source of the material is acknowledged and any reproduction of the whole or substantial parts of this document must include this notice.

Version 4.0
29.04.10

Contents

A – Introduction and summary of approach 1
A1. Introduction 1
A2. The data protection principles 2
A3. Summary of approach 3

Step 1 – Will there be a transfer of personal data to a third country? 4
1. International data transfers 4
1.1 What does the legislation say? 4
1.2 The Directive 4
1.3 Are all international movements of data covered? - Transfer or transit? 4

Step 2 – Does the third country and the circumstances of the transfer ensure an adequate level of protection? 7
2. Adequate level of protection 7
2.1 Is there an 'adequate level of protection'? 7
2.2 Community findings of adequacy 7
2.3 Assessing adequacy 8
2.4 Adequacy test – general adequacy criteria 10
2.5 Legal adequacy criteria 12
2.6 Proceed with transfer? 14

Step 3 – Have or can the parties put into place adequate safeguards? 15
3. Adequate safeguards 15
3.1 Use of model clauses or binding corporate rules 15
3.2 Model clauses 16
3.3 Binding corporate rules 18
3.4 Proceed with transfer? 21

Step 4 – Do any other derogations to the eighth principle apply? 23
4.1 The derogations 23
4.2 Consent 24
4.3 Necessary for a contract between data controller and data subject or data controller and third party 24
4.4 Substantial public interest 25
4.5 Legal matters 26
4.6 Vital interests of the data subject 26
4.7 Public registers 27
4.8 Proceed with transfer? 27

5. International outsourcing to data processors located in a third country 28

Data Protection Act 1998

The eighth data protection principle and international data transfers

A – Introduction and summary of approach

A1. Introduction

A1.1 This guidance considers the provisions of the eighth data protection principle (the eighth principle) of the Data Protection Act 1998 (the Act) relating to international transfers of personal data[1] made by a data controller based in the UK to recipients based outside the European Economic Area (see 1.1.2 below). Where transfers outside of the EEA originate from other European Member States, the advice and guidance of the relevant data protection authority ('DP authority') in those countries should always be sought as the implementation of the Directive and its interpretation by these other DP authorities varies.

A1.2 The views of the Information Commissioner (the Commissioner) are informed by continuing discussions with international businesses, fellow EU Data Protection Commissioners and non-EU authorities. This guidance and the Commissioner's website will be amended from time to time to reflect any developments in this area including any future Community findings as to which countries give adequate protection for the purposes of the eighth principle.

A1.3 This recommended approach is intended to replace the preliminary analysis on international data transfers published in July 1999.

A1.4 To the extent that the Commissioner is required to examine any transfer in the context of the eighth principle, he will expect to see evidence that the data controller making the transfer has followed the approach and the various criteria set out in this guidance.

[1] For guidance as to what constitutes personal data and on other defined terms in the Act (such as 'data controller', 'data processor' and 'data subject'), please see our website (www.ico.gov.uk).

A2. The data protection principles

A2.1 There are eight data protection principles (the principles) in the Act with which data controllers are required to comply. These are sometimes referred to as the principles of 'good information handling'. Except to the extent that a data controller is able to claim an exemption from any of the principles they will apply to all personal data processed by a data controller. The principles are set out in Schedule 1 to the Act[2].

A2.2 This guidance is concerned only with the eighth principle but it should be remembered that data controllers transferring personal data are required to comply with the principles and the Act as a whole.

A2.3 In addition, before making a transfer of personal data, a data controller should consider whether it is possible for it to achieve its objectives without processing personal data at all and examine options such as the anonymisation of such data. If the data does not relate to identifiable individuals then this brings such data outside the scope of the Act and means that any transfer could be made freely and without reference to the eighth principle.

[2] Please see the Commissioner's guidance - '*The Guide to Data Protection*' for guidance on all the Principles and the Act as a whole (http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx).

A3. Summary of approach

A3.1 The structure of this guidance follows the Commissioner's good practice approach to transfers of personal data outside of the EEA. Namely:

- **Step 1** - consider whether there will be a **transfer of personal data to a third country**. See Step 1 below.

- **Step 2** – consider whether the third country and the circumstances surrounding the transfer ensure that an **adequate level of protection** will be given to that data. See Step 2 below.

- **Step 3 –** consider whether the parties have or can put into place **adequate safeguards** to protect that data (for instance, by entering into model clauses or establishing binding corporate rules). See Step 3 below.

- **Step 4 –** consider if any of the **other derogations** to the eighth principle specified in the Act apply (such as the consent of the data subject to the transfer). See Step 4 below.

A3.2 In addition, section 5 expands on some of these issues in the context of **international outsourcing to data processors** and its interaction with the eighth principle.

Step 1 – Will there be a transfer of personal data to a third country?

1. International data transfers

1.1 What does the legislation say?

1.1.1 The eighth principle provides that:

"Personal data shall not be transferred to a country or territory outside the European Economic Area 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".[3]

1.1.2 The European Economic Area (the EEA) consists of the EU Member States together with Iceland, Liechtenstein and Norway. Any other country or territory is considered to be a 'third country' for the purposes of the eighth principle.

1.2 The Directive

1.2.1 The eighth principle is derived from a requirement in the European Communities Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data (the Directive). Article 25(1) of the Directive, requires that:

"The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if …the third country in question ensures an adequate level of protection."

1.3 Are all international movements of data covered? - Transfer or transit?

1.3.1 Once it has been established that it will be necessary to process personal data and that it will be going out of the EEA to a third country, the next

[3] Part 1 of Schedule 1 to the Act

question to ask is whether this movement of data represents a 'transfer' for the purposes of the eighth principle.

1.3.2 The Act does not define 'transfer' but the ordinary meaning of the word is transmission from one place, person, etc to another. Transfer does not mean the same as mere transit. Therefore the fact that the electronic transfer of personal data may be routed through a third country on its way from the UK to another EEA country does not bring such transfer within the scope of the eighth principle.

1.3.3 Section 1(3) of the Act requires that the transfer of information which is not initially personal data but is intended to be processed automatically or as part of a 'relevant filing system'[4] only *after* it has been transferred should be afforded the protection of the Act. An example of this would be where information is provided by someone in the UK over the telephone to someone in a third country who then enters the information on a computer.

1.3.4 In the case of Bodil Lindqvist v Kammaraklagaren (2003) *(*Case C-101/01), the European Court of Justice held that there was no transfer of personal data to a third country where an individual loaded personal data onto an internet page in a Member State using a internet hosting provider in that Member State, even though the page was accessible via the internet by people based in a third country. Instead, a transfer was only deemed to have taken place where the internet page was actually accessed by a person located in a third country. In practice, data are often loaded onto the internet with the intention that the data be accessed in a third country, and, as this will usually lead to a transfer, the principle in the Lindqvist case will not apply in such circumstances. However, in situations where there is no intention to transfer the data to a third country and no transfer is deemed to have taken place as the information has not

[4] Section 1(1) of the Act – see part A3 of 'The Guide to Data Protection' for an explanation of the definition of 'relevant filing system' (http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx).

been accessed in a third country (ie the eighth principle does not apply), data controllers will still need to ensure that the processing complies with all of the other principles. In particular, data controllers must consider the requirement in the first data protection principle that the processing must be fair which may be contravened by making the data so widely accessible.

Step 2 – Does the third country and the circumstances of the transfer ensure an adequate level of protection?

2. Adequate level of protection

2.1 Is there an 'adequate level of protection'?

2.1.1 Having established that there is a transfer of personal data to a third country, the data controller must then ask whether that third country ensures an adequate level of protection to the personal data taking into account all the circumstances of the transfer ('adequacy').

2.1.2 A decision of whether or not there is adequacy may be based on a Community finding of adequacy (see 2.2 below) or after an assessment of adequacy made by the data controller itself (see 2.3 below).

2.2 Community findings of adequacy

2.2.1 Article 25(6) of the Directive (and Schedule 1, Part II, Para 15 of the Act) requires that, where the European Commission (the Commission) has made a finding that a third country does, or does not, ensure adequacy, any question as to whether there is adequacy will be determined in accordance with that finding.

2.2.2 As at April 2010, the Commission has made positive findings of adequacy in relation to the following countries.[5]

- Argentina
- Canada[6]
- Guernsey
- Isle of Man
- Switzerland
- Jersey

[5] An up-to-date list of Community findings is available at http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm and http://www.ico.gov.uk/what_we_cover/data_protection/international/international_transfers.aspx

[6] In relation to recipients subject to the Canadian Personal Information Protection and Electronic Documents Act (PIPED Act).

- Faroe Islands

2.2.3 In addition to findings relating to the above countries, the Commission has also made a finding regarding specific transfers to the United States of America by the use of Safe Harbor.

2.2.4 Safe Harbor

The Safe Harbor scheme consists of a set of principles which are similar to the principles found in the Act[7] and relates to transfers to US entities. It has been operational since 1 November 2000 when the US Department of Commerce opened the on-line self certification process for US organisations wishing to notify their adherence to the principles. The scheme creates a voluntary mechanism enabling US organisations to qualify as offering adequate protection for personal data transferred to them from the EU and is recognised by the Commission as providing adequate protection for the transfer of personal data under the terms of the Directive.

2.2.5 The Federal Trade Commission is primarily responsible for enforcing Safe Harbor but the scheme is not available to companies in all sectors, e.g. telecommunications companies and financial institutions are not covered by the regime. A full list of companies that have signed up to the Safe Harbor regime can be found on the US Department of Commerce's Safe Harbor website[8].

2.3 Assessing adequacy

2.3.1 Where the data protection regime in the third country has not been subject to a Commission finding of adequacy, it is for exporting controllers to assess adequacy in a way which is consistent with the Directive and the Act. In carrying out this assessment of adequacy, the Commissioner would expect exporting controllers to be able to demonstrate how they have addressed the various criteria set out in this guidance.

[7] http://www.export.gov/safeharbor/index.html
[8] http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

2.3.2 In the Directive, the basis of any assessment of adequacy is contained in Article 25(2), which states:

"The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."

2.3.3 Article 25(2) has been implemented by the Act[9] at Schedule 1, Part II paragraph 13 which states that the level of protection must be "adequate in all the circumstances of the case" and provides that, in assessing adequacy, particular consideration should be given to:

- the nature of the personal data;
- the country or territory of origin of the information contained in the data;
- the country or territory of final destination of that information;
- the purposes for which and period during which the data are intended to be processed;
- the law in force in the country or territory in question;
- the international obligations of that country or territory;
- any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases); and
- any security measures taken in respect of the data in that country or territory.

[9] Part II of Schedule 1, paragraph 13

2.3.4 The above adequacy criteria, for the purposes of this guidance, are divided into two categories – the '**general adequacy criteria**' and the '**legal adequacy criteria**'. The general adequacy criteria (described in more detail in 2.4 below) are factors which the exporting data controller will be able to identify easily; for example, the nature of the personal data being transferred and purpose for which the data are to be processed. General adequacy criteria should be assessed in detail on every occasion. The legal adequacy criteria (see 2.5 below), may be more difficult for the controller to assess as they are factors relating to the legal system in force in the third country.

2.3.5 An exhaustive analysis of the legal adequacy criteria may be unnecessary if an assessment of the general adequacy criteria has revealed that in the particular circumstances the transfer is low risk. Conversely, if the general adequacy assessment reveals a high risk transfer (e.g. if the data is particularly sensitive), then a more comprehensive investigation of the legal adequacy criteria will be expected.

2.4 Adequacy test – general adequacy criteria

2.4.1 As stated in 2.3.4 above, the 'general adequacy criteria' should be assessed in every case as the information will be in the knowledge of the exporting controller and therefore relatively straightforward to assess. These are:

- the nature of the personal data;
- the purpose(s) of the proposed transfer;
- the period during which the data are intended to be processed;
- any security measures taken in respect of the data in the third country;
- the country of origin of the personal data; and
- the country of final destination of the personal data.

2.4.1.1 The nature of the personal data

The transfer of some types of personal data will pose little risk to the rights and freedoms of individuals. For instance, the transfer of a list of internal telephone extensions to overseas subsidiaries of a multinational company would not be considered to be high risk as it is unlikely that the data subject would suffer significant damage if his business telephone number was obtained by an unauthorised source. Conversely, if an exporting controller is proposing to transfer sensitive personal data such as health records, the threshold of protection required in order for it to be adequate will clearly be higher.

2.4.1.2 The purposes for which the data are intended to be processed

Some purposes for which data are processed will carry greater risks to the rights of the individuals than others. For instance, if the data are processed for internal purposes only (such as for an internal company telephone list as described above) this may carry with it less risk than if the details were more widely distributed, for instance in marketing brochures or on an internet site.

2.4.1.3 The period during which the data are intended to be processed

If the data are only going to be processed once or for a short time and then destroyed, then the risks arising from any lack of protection may be less than if the data are being processed on a long-term basis.

2.4.1.4 Any security measures taken in respect of the data in the third country

Exporting controllers may be able to ensure that the personal data are secure from any outside interference by means of, for example, technical measures such as encryption or the adoption of information security management practices analogous to those in ISO17799/BS7799. In practice, security is often a key factor in the commercial considerations of the parties.

2.4.1.5 The country or territory of origin of the information contained in the data

This is not necessarily the same as the country or territory from where the transfer originates but rather the country or territory from which the

data originate. In most cases this is likely to be the country or territory from where the information was originally obtained. Note that where the information has been obtained in a third country, this will be a relevant factor to consider because the data subject may have different expectations as to the level of protection that will be afforded to their data than they would have had if the information had been obtained in the EEA. Where a third country is the country (or territory) of origin of the information contained in the data, the Act is not intended to provide a different level of protection to a citizen of that country (or territory) than is provided by the data protection regime, if any, in the country (or territory) of origin.

2.4.1.6 The country or territory of final destination of that information

This is not necessarily the same as the destination country in relation to the particular transfer in question. In some cases it is known that there will be a further transfer to another country or territory which may or may not be outside the EEA. If this is the case, then the protection given in that ultimate destination will be relevant in assessing adequacy.

2.5 Legal adequacy criteria

2.5.1 These are criteria that relate particularly to the third country in question. Namely:

- the law in force in the third country;
- the international obligations in that third country; and
- any relevant codes of conduct or other rules which are enforceable in that country or territory.

2.5.2 As discussed above, the extent to which exporting controllers conduct an exhaustive analysis of the legal adequacy criteria will be for them to assess in the light of all the circumstances of the case and their assessment of the general adequacy criteria discussed in 2.4 above.

2.5.3 Even in those cases where they do not conduct an exhaustive analysis, exporting controllers will be expected to be able to recognise countries where there would be real danger of prejudice because of, for example, instability in the third country at the time of the transfer, and they will be expected to assess this danger in light of the general adequacy criteria.

2.5.4 An example of a situation where an exporting controller might reasonably be expected to have undertaken a detailed analysis of the legal adequacy criteria would be where the exporting controller is proposing to set up a permanent operation in a third country and anticipates making regular, large-scale transfers to that country. Conversely, where the data transferred have a low level of sensitivity, such as the internal telephone list example discussed in 2.4 above, an exhaustive legal adequacy test may not be necessary.

2.5.5 When legal adequacy is assessed, an exporting controller should consider, in particular, the following questions.

- Has the third country adopted the OECD Guidelines[10] and, if so, what measures has it taken to implement them?
- Has the third country ratified Convention 108[11] and are there appropriate mechanisms in place for compliance with it?
- Does the third country have a data protection regime in place which meets the standards set out in the Article 29 Working Party document adopted on 24 July 1998 (WP 12)[12]
- Does the third country have any legal framework for the protection of the rights and freedoms of individuals generally?

[10] 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' – Organisation for Economic Co-operation and Development, 1980

[11] Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data, Strasbourg 1981

[12] 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' - Article 29 Working Party (DGXV D/5025/98 WP 12). This sets out certain principles - such as the 'purpose limitation principle', the 'transparency principle' and the 'security principle' - which the Working Party believe should be embodied in a data protection regime in order for it to be considered to be adequate.

- Does the third country recognise the general rule of law and, in particular, the ability of parties to contract and bind themselves under contracts?
- More specifically, are there laws, rules or codes of practice (general or sectoral) which govern the processing of personal data?

2.6 Proceed with transfer?

2.6.1 If adequacy is established further to either (i) a Community finding of adequacy or (ii) the data controller's adequacy assessment, then the transfer can proceed from the UK to the third country in compliance with the eighth principle. Note that if transfers are taking place from more than one European jurisdiction then local advice should always be sought as there may be different requirements which apply depending on the jurisdictions in question.

2.6.2 If adequacy is not established under (i) or (ii) above then the exporting controller should proceed to Step 3 and examine the suitability of implementing the adequate safeguards described.

Step 3 – Have or can the parties put into place adequate safeguards?

3. Adequate safeguards

3.1 Use of model clauses or binding corporate rules

3.1.1 If it is not possible for an exporting data controller to satisfy itself that there is adequacy (as described in Part 2 above), the use of Commission-authorised standard contracts (model clauses) or specific, approved binding corporate rules (BCR) enable the transfer to be made exempt from the restrictions of the eighth principle on the basis that the model clauses or set of BCR provide adequate safeguards for the rights and freedoms of data subjects. This derives from Article 26(2)[13] of the Directive which states that:

"a Member State may authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection…where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses…"

3.1.2 Transfers which are exempt by virtue of Article 26(2) ensure conditions whereby the individuals in question continue to be protected as regards processing of their data even after the data have been transferred. For this reason, it is good practice to attempt to satisfy one of these Article 26(2) derogations before considering the derogations which derive from Article 26(1)[14] (which do not ensure such a high level of protection - see Step 4 below).

[13] Implemented by paragraphs 8 and 9 of Schedule 4 to the Act.
[14] Implemented by paragraphs 1 to 7 of Schedule 4 to the Act.

3.2 Model clauses

3.2.1 Further to Article 26(4) of the Directive, the Commission is empowered to recognise standard contractual clauses as offering adequate safeguards for the purposes of Article 26(2) and it has approved model clauses further to the following decisions.

- Commission Decision 2001/497/EC[15], dated 15 June 2001 – in which the Commission approved model clauses for transfers from data controllers in the EEA to data controllers outside the EEA (Set I controller-controller).

- Commission Decision 2002/16/EC[16], dated 27 December 2001 – in which the Commission approved model clauses for transfers from data controllers in the EEA to data processors outside the EEA (controller-processor).

- Commission Decision 2004/915/EC[17], dated 27 December 2004 – in which the Commission approved an alternative set of model clauses for transfers from data controllers in the EEA to data controllers outside the EEA (Set II controller-controller).

3.2.2 The Commissioner has issued authorisations under s54(6) of the Act in relation to each of the model clauses (on 21 December 2001, 8 March 2003 and 27 May 2005, respectively) providing that, for the purpose of paragraph 9 of Schedule 4 to the Act, the eighth principle does not apply where the transfer has been made using any of the model clauses. This means that an exporting controller who uses these model clauses does not need to make a separate assessment of adequacy in relation to the transfer.

---

[15] The clauses are an annex to the Decision which approves them.
http://eur-lex.europa.eu/pri/en/oj/dat/2001/l_181/l_18120010704en00190031.pdf
[16] The clauses are an annex to the Decision which approves them.
http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_006/l_00620020110en00520062.pdf
[17] The clauses are an annex to the Decision which approves them.
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00740084.pdf

3.2.3 The model clauses contain obligations on both the data exporter and data importer to ensure that the transfer complies with the standards required by the Directive and the data subject has a right to directly enforce its rights under them. Under the Set I controller-controller model clauses, the data exporter and data importer are jointly and severally liable to the data subject for any damage it suffers as a result of a breach by either party of those of the model clauses under which the data subject is a beneficiary (third party beneficiary clauses). This differs from the Set II controller-controller model clauses under which the data subject can only enforce its rights against the party who is responsible for the relevant breach[18]. Under the controller-processor model clauses, the data exporter is liable to the data subject for any breach by either party of the third party beneficiary clauses except in limited circumstances. However, if the breach was caused by the data importer, the data importer is required to indemnify the data exporter to the extent of its liability to the data subject.

3.2.4 In addition to the greater flexibility inherent in the Set II controller-controller model clauses, these clauses also give the data importer greater discretion in deciding how to comply with data protection laws and how to respond to subject access requests. However, it should be noted that: "to prevent abuses with this additional flexibility…data protection authorities can more easily prohibit or suspend data transfers based on the Set II controller-controller model clauses in those cases where the data exporter refuses to take appropriate steps to enforce contractual obligations against the data importer or the latter refuses to cooperate in good faith with competent supervisory data protection authorities." [19]

3.2.5 None of the versions of the model clauses may be amended but the parties are free to include any other clauses on business related issues provided that they do not contradict the model clauses. Indeed, the Set II controller-controller model clauses include some suggested commercial

[18] Note that under Set II the data importer must provide the data exporter with satisfactory evidence of its ability to meet its liabilities with details of any insurance coverage etc (section 1(f) of the Set II controller-controller model clauses).
[19] Paragraph 7 of the Commission Decision 2004/915/EC dated 27 December 2004

clauses to be incorporated (e.g. an indemnity provision, dispute resolution clause and extra termination right). The Set II controller-controller clauses also allow the parties to update the description of the transfer that the parties will have originally set out in Annex B, to reflect changes as the relationship develops.

3.2.6 Use of any of versions of the model clauses, whether as a stand-alone contract or incorporated into another contract, where the wording is changed but without altering the intended meaning or effect of any clause, does **not** amount to use that is authorised by the Commissioner under paragraph 9 of Schedule 4 to the Act. However, this does not prevent the data controller from taking the view that the transfer is made on terms which provide adequacy (as defined in 2.1.1 above), and indeed the use of different terms with the same meaning or effect as those in the model terms would be a significant factor were the Commissioner required to assess the adequacy of any protection given to the data.

3.2.7 Note that if the only change to the model clauses is to make the contract between more than two parties (e.g. where there is more than one data importer) rather than remain a bilateral agreement between one data exporter and importer then the Commissioner is of the view that this **does** remain within the scope of the Commissioner's authorisation provided that the obligations of all the parties remain clear and legally binding.

3.3 Binding corporate rules (BCR)

3.3.1 BCR are internal codes of conduct operating within a multinational organisation for the purposes of enabling transfer of data outside the EEA (but within the group) to be made on a basis which ensures adequate safeguards for the rights and freedoms of data subjects for the purposes of paragraph 9 of Schedule 4 to the Act. They are designed to be a global solution for multinational companies by ensuring their intra-group transfers comply with the eighth principle and providing a simple mechanism for obtaining the necessary authorisations across the EU (see 3.3.4 below). BCR must be submitted for approval by the Commissioner in order to

obtain an authorisation which provides that transfers from the UK may be made within the group on the basis of the BCR (further details of the authorisation process is set out in 3.3.3 below).

3.3.2 The concept of using BCR to create adequate safeguards for the purposes of Article 26(2) was devised by the Article 29 Working Party in its working document on binding corporate rules, adopted on 3 June 2003 (WP74)[20]. Subsequently, to assist with compliance, the Article 29 Working Party has developed the following documents.

- Model checklist on the content of a BCR application to DP authorities (model checklist). [21]
- Co-operation procedure to facilitate the authorisation process (the co-operation procedure).[22]
- Standard application form based on the model checklist (the application form). [23]
- Table of BCR requirements (this is a summary of WP 74 and WP 108 in an easy-to-follow table format). [24]
- Framework BCR (a suggestion of what a BCR application might look like). [25]
- BCR FAQs - a working document that is constantly being updated in the light of new questions and experience. [26]

[20] Working document (WP 74) Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 11639/02/EN WP 74
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf.
[21] Working document (WP 108) Establishing a Model Checklist Application for Approval of Binding Corporate Rules 05/EN WP 108 – adopted 14 April 2005
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf
[22] Working document (WP 107) Setting forth a co-operation procedure for issuing common opinions on adequate safeguards resulting from binding corporate rules 05/EN WP 107 – adopted 14 April 2005
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp107_en.pdf
[23] Recommendation 1/2007 (WP 133) on the standard application for approval of binding corporate rules for the transfer of personal data - adopted 10 January 2007
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp133_en.doc
[24] Working document (WP 153) setting up a table with the elements and principles to be found in BCR 1271-00-00/08/EN WP 153 - adopted 24 June 2008
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp153_en.pdf
[25] Working document (WP 154) setting up a framework for the structure of BCR 1271-00-01/08/EN WP 154 - adopted 24 June 2008
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp154_en.pdf

3.3.3 Applications for the authorisation of BCR to the Commissioner must be made in accordance with the application form and applicants will be required to demonstrate that adequate safeguards are in place within the organisation and must include:

- evidence that the measures are binding, both internally and externally;
- details of a data protection audit plan;
- a description of processing and flows of information;
- a description of the data protection safeguards in place; and
- details of a mechanism for reporting and recording changes.

The Commissioner will only give an authorisation where he is satisfied that such adequate safeguards can be delivered.

3.3.4 Where a data controller wishes to use BCR to export data out of the EEA from a number of different European jurisdictions, WP 74 provides a mechanism whereby the exporting data controller can, in the first instance, deal with one DP authority who then co-ordinates the authorisation process from other DP authorities in all the other European jurisdictions in which that company operates. For this purpose, the data controller will need to propose the DP authority in one jurisdiction as the 'lead authority' who will then liaise with the other relevant DP authorities in accordance with the co-operation procedure with a view to getting the BCR approved by them all[27]. The co-operation procedure suggests that the decision on which DP authority should be the 'lead authority' should be based on criteria such as the location:

- of the group's European headquarters;
- of the company within the group that has delegated data protection responsibilities;

[26] Working document (WP 155) on frequently asked questions related to BCR 1271-00-02/08/EN WP 155 rev.01 - adopted on 24 June 2008; revised on 1 October 2008 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp155_en.pdf

[27] However, the Data Protection Authorities may among themselves decide to allocate the lead authority to another Data Protection Authority than the one proposed by the applicant

- of the company within the group best placed to deal with the application and enforce the BCR;
- where most decisions are taken in relation to the processing; and
- where the most transfers outside the EU take place.

3.3.5 Some DP authorities have signed up to a policy of mutual recognition where they have agreed to authorise the BCR without further comment or amendment at the point at which it is circulated by the lead authority with an opinion that it provides an adequate level of protection as described in the working party documents. At this point not all DP authorities in the EEA have signed up to this policy and so the co-operation procedure will still be used in many cases alongside mutual recognition.

3.3.6 Once a set of BCR have been approved by the DP authorities as part of the co-operation procedure or as a result of mutual recognition, and any national permits obtained and necessary notifications made, transfers falling within their scope can take place from the countries from which authorisations have been received, provided it is for a purpose and in a manner that is compliant with any national data protection or other relevant laws in that country.[28]

3.3.7 The Commissioner's website contains details of the BCR which it has approved and further information as to how to make an application for the authorisation of BCR[29].

3.4 Proceed with transfer?

3.4.1 If the model clauses are used, or the Commissioner has approved a set of BCR which would govern the transfer, the transfer from the UK to a third country can take place without further authorisation. However, if neither of these methods is appropriate in relation to the transfer and the exporting

[28] Although transfers made under intra-group codes which have not been submitted for approval by the Commissioner as BCR will not be exempt from the eighth principle, such codes may enable data controllers to establish adequacy as part of any adequacy assessment they carry out as described in Part 2 to this guidance.
[29] http://www.ico.gov.uk/what_we_cover/data_protection/international/international_transfers.aspx

controller is unable to adduce adequacy further to Step 2 then it should consider whether any further derogations apply, as described in Step 4.

Step 4 – Do any other derogations to the eighth principle apply?

4.1 The derogations

4.1.1 As set out in Part 3 above, the use of BCR and model clauses are two derogations from the eighth principle derived from Schedule 4 of the Act. There are also a number of other derogations in Schedule 4 which may be considered. They are as follows.

- The data subject has consented to the transfer.
- The transfer is necessary for the performance of, or for the taking of steps at the request of the data subject with a view to entering into, a contract between the data subject and the data controller.
- The transfer is necessary for the performance of, or entering into, a contract between the data controller and a third party entering into the contract at the request, or in the interests, of the data subject.
- The transfer is necessary for reasons of substantial public interest.
- The transfer is necessary in connection with legal proceedings, advice or rights.
- The transfer is necessary to protect the vital interests of the data subject.
- The transfer is of part of the personal data on a public register.[30]

4.1.2 Each of these derogations is discussed in more detail in 4.2 to 4.7 below. Unlike BCR or model clauses, where these derogations are used there is not necessarily any protection in place in relation to the data being transferred. Instead, these provisions reflect the fact that there are instances where it will be justifiable to transfer data even though there will be a lower level of protection given to those data. As such, in interpreting these provisions, the derogations should be narrowly construed.

4.1.3 In addition, when applying the derogations, exporting controllers should be aware that just because the eighth principle does not apply, it does not mean that the other seven principles do not apply to the data and these

[30] Schedule 4, paras 1-7 (equivalent to Article 26(1) of the Directive).

should always be considered in addition to the eighth principle in the context of international data transfers.

4.2 Consent

4.2.1 Article 2(h) of the Directive defines consent as "any freely given specific and informed indication of [the data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed". Consequently, exporting controllers should be able to produce clear evidence of the data subject's consent in any particular case and may be required to demonstrate that the data subject was informed as required. Similarly, valid consent means that the data subject must have a real opportunity to withhold their consent without suffering any penalty, or to withdraw it subsequently if they change their mind. This can be particularly relevant if it is employee consent which is being sought. For these reasons, consent is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or structural transfers of data to a third country. As the Article 29 Working Party states in its paper on the interpretation of Article 26(1): "relying on consent may…prove to be a 'false good solution', simple at first glance but in reality complex and cumbersome".[31]

4.3 Necessary for a contract between data controller and data subject or data controller and third party

4.3.1 In order to fall within these two derogations it needs to be shown that the transfer is *necessary* for the performance or entering into of the contract. If it is a third party entering into the contract, rather than the data subject, then it has to be clearly shown that they are entering into it at the request of the data subject or that it is clearly in the data subject's interests.

4.3.2 An example given by the Article 29 Working Party[32] of a contract that falls within this category is where there is a transfer to a third country by travel

[31] Article 29 Working Party's Working document on a common interpretation of Article 26(1) of Directive 95/46/EC (2093/05/EN – WP114) page 11
[32] Ibid., page 13

agents of personal data of their clients to hotels or to other commercial partners that will organise the clients' stay. This is contrasted with the transfer of employee data from an EEA subsidiary to a non-EEA parent company in order to centralise a multinational group's HR and payment functions which, it has been argued, is necessary for the data subject's employment contract with the data controller. Although such a transfer may provide a cost-efficiency which may indirectly benefit the employee, it would be difficult to show that the centralisation of payment functions is objectively *necessary* for the performance of the data subject's employment contract and could not be carried out elsewhere. Therefore it is likely that in these circumstances the derogation would not apply. Note that this does not mean that this arrangement is not permitted at all – for instance, it may satisfy the adequacy criteria discussed in Step 2 and comply with the eighth principle under those grounds – merely that this particular derogation is unlikely to be applicable in these circumstances.

4.3.3 Similarly, where the contract is between the data controller and a third party, not only does the data controller need to show that the transfer is necessary for that contract, unless the contract has been entered into at the data subject's request, the data controller needs to show "a close and substantial connection between the data subject's interests and the purpose of the contract".[33] This derogation is discussed further in the context of outsourcing in 5.8 below.

4.4 Substantial public interest

4.4.1 To qualify for this derogation, the transfer must be "necessary for reasons of substantial public interest".[34] This is subject to the same strict interpretation as that applied to the other derogations discussed in this section and is a high threshold. The Secretary of State may by order specify circumstances in which a transfer is to be taken to be necessary for reasons of substantial public interest. No such orders are in force to date.

[33] Ibid., page 14.
[34] Schedule 4, para 4(1)

4.4.2 Recital 58 of the Directive gives examples of cases where international exchanges of data might be necessary "between tax or customs administrations in different countries" or "between services competent for social security matters". The transfer should be in the public interest in the Member State itself rather than the third country.

4.5 Legal matters

4.5.1 This derogation will apply where the transfer is necessary:

- for the purpose of, or in connection with, any legal proceedings[35] (including prospective legal proceedings);
- for the purpose of obtaining legal advice; or
- for the purposes of establishing, exercising or defending a legal right.

Once again, the emphasis in using this derogation is on necessity and the need to balance the legal rights at the centre of the advice or action with the data subject's rights in relation to their personal data.

4.5.2 An example given by the Article 29 Working Party of where this derogation may apply would be where a parent company based in a third country is sued by an employee of the group based at one of the European subsidiaries, and the company requests the European subsidiary to transfer certain data relating to the employee if the data are necessary for the defence.[36]

4.6 Vital interests of the data subject

The Commissioner considers that this exception to the eighth principle may only be relied upon where the data transfer is necessary for matters of life and death such as a medical emergency. For instance, it would clearly be essential to be able to transfer data if the data subject is in urgent need of medical attention in a third country and only their usual doctor based in a Member State can supply this data. The derogation

[35] Including legal proceedings outside the UK (e.g. in the third country)
[36] Op cit. page 15

could not be relied upon, by contrast, if the data are not transferred for the purpose of treating the data subject but instead are to be used for general medical research in the future.

4.7 Public registers

This derogation may be relied upon if the transfer is of part of the personal data on a public register in a Member State and any conditions to which the register is subject are complied with by any person to whom the data are or may be disclosed after the transfer. Note that the data transferred should only be of part of the data and "not involve the entirety of the data or entire categories of the data contained in the register".[37]

4.8 Proceed with transfer?

4.8.1 If the transfer falls under any of the derogations discussed above then it is exempt from the eighth principle and may proceed without any further requirements or prior authorisation. However, if adequacy has not been adduced in line with Step 2 or the derogations described in Steps 3 and 4 do not apply, the transfer may not proceed without being in breach of the eighth principle. Remember also that compliance with the eighth principle is only one aspect of satisfying the requirements of the Act and a data controller should ensure that it complies with all the principles when processing and transferring personal data.

4.8.2 The final part of this guidance, section 5, deals with issues which may arise in relation to a particular type of data transfer – namely, transfers to data processors located in a third country – and provides further illustration of how the eighth principle operates in practice.

[37] Recital 58 of the Directive.

5. International outsourcing to data processors located in a third country

5.1 Increasingly, UK data controllers are using data processors[38] in third countries to carry out processing on their behalf. A transfer to a data processor in a third country will be caught by the eighth principle.

5.2 Where a transfer is made to a data processor in a third country by a UK data controller, the exporting controller remains the data controller in the UK for the purposes of the Act. This means that the data controller remains subject to the Commissioner's powers of enforcement and is responsible for protecting individuals' rights under the Act in relation to the overseas processing of the personal data by the data processor.

The seventh principle

5.3 Where there is a transfer to a data processor, wherever that processor is located, a data controller must comply with the requirements of all the principles, including the seventh data protection principle (the seventh principle) which states that:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

5.4 The seventh principle (at paragraph 11 of Part II of Schedule 1 to the Act) requires that where a third party undertakes processing on behalf of a data controller, that data controller must:

(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and

[38] Defined in section 1(1) of the Act.

(b) take reasonable steps to ensure compliance with those measures (such as conducting regular audits and reviews).

In addition, a data controller will not be regarded as complying with the seventh principle unless the processing is carried out under a contract "made or evidenced in writing"[39], and under which the data processor is to act only on instructions from the data controller and which contains an obligation on the part of the data processor to comply with provisions equivalent to those imposed on a data controller by the seventh principle.

Use of model clauses and assessment of adequacy

5.5 One form that such a contract "made or evidenced in writing" may take is the data controller-data processor model clauses discussed in 3.2 above which have been approved by the Commission as offering adequate safeguards for the purposes of Article 26(2).[40] The use of these terms can simultaneously satisfy the requirement for a contract in the seventh principle and fall under a derogation from the eighth principle and, for that reason, may be attractive in data controller-data processor international outsourcings.

5.6 However, a data controller in the UK need not necessarily use these controller-processor model clauses when entering into a contract with a data processor in a third country provided that any contractual arrangement satisfies the requirements of the seventh principle and the data controller has successfully complied with, or derogated from, the eighth principle by another means. The model clauses are merely one method of addressing the requirements of the eighth principle and there are many other methods which have been discussed in this guidance which may be more appropriate in the circumstances.

[39] Schedule 1, Part II, paragraph 12(a)(i).
[40] Commission Decision 2002/16/EC dated 27 December 2001

5.7 In particular, the model clauses will not be necessary if the data controller establishes that there is adequacy as described in Step 2 of this guidance. In this respect, the Commissioner's guidance is that compliance with the seventh principle will go some way towards satisfying the adequacy requirements of the eighth principle (given the continuing contractual relationship between the parties and the data controller's continued liability for data protection compliance under the Act). However, the Commissioner would still expect the data controller to make due diligence checks in relation to the data processor and conduct some examination of the type of matters usually looked at in relation to adequacy (e.g. the nature of the data, the country in which the data processor is located and the security arrangements in that third country).[41] If such due diligence and analysis did not reveal any particular risks in relation to the transfer, then the controller-processor relationship and the security measures implemented further to compliance with the seventh principle would be likely to ensure adequacy and, therefore, the transfer would be able to proceed in compliance with the eighth principle.

Use of "necessary for contract in the interests of data subjects" derogation

5.8 As discussed at 4.3.3 above, there is a derogation from the eighth principle where the transfer is necessary for the conclusion or performance of a contract between the data controller and a person other than the data subject where such a contract is entered into at the data subject's request or is in the interests of the data subject.[42] It is sometimes argued by data controllers that a transfer which is necessary for an outsourcing contract with a service provider in a third country will fall under this derogation where the subject of the contract is indirectly in the interests of the data subjects (for instance, where the service provider is administering the data controller's payroll functions). The argument advanced is that as the contract relates to the pay of the data subject (the employee) then it is in the interests of the data subject that this contract is

[41] See Step 2.4 and 2.5 for all the adequacy criteria to be taken into account when adducing adequacy.
[42] Paragraph 3 of Schedule 4 to the Act.

performed. However, the Commissioner (in common with the Article 29 Working Party[43]) does not support this view on the basis that there is not a sufficiently close and substantial link between the contract and the data subject's interests. Instead the Commissioner would, as a general rule, expect such arrangements to comply with, or be exempt from, the eighth principle through other means – such as the adducing of adequacy (as described in Step 2) or the implementation of adequate safeguards (as set out in Step 3 and 5.7 above).

Subprocessors

5.9 Many transfers to a third country are made where a data processor based in the UK then subcontracts the processing to another processor outside the EEA. As the data controller will remain liable for compliance with the Act, it will be for the data controller to satisfy itself that such subcontracting will not materially increase the risks to the data being processed. In this situation, the data controller must expressly permit the subcontracting and it is likely that this will be best achieved by means of a clause in the controller to processor contract. The controller to processor contract should also contain an obligation on the part of the processor to contract in equivalent terms with the subprocessor and to enforce the terms of the subprocessor contract. Any contract between the processor and the subprocessor should therefore mirror the main controller to processor contract and also address any adequacy issues not covered by the main controller-processor contract (in the event that the main contract was drafted in the context of a processing within the UK).

5.10 As the data controller in the UK always remains liable to enforcement action by the Commissioner and to a civil action by a data subject for breaches taking place outside the UK as a result of the acts of a data processor, it is particularly important that a data controller is satisfied as to the identity and propriety of both the processor and any subprocessor

[43] See pages 13-14 of WP 114 – op. cit

engaged and, in particular, that the requirements of the seventh principle are satisfied.

General points

5.11 Data controllers should take into account the legislation in place in the country or territory where the chosen processor is located and any obligations this may impose, for example, the US PATRIOT Act. As part of the assessment as to the adequacy of the protection available for the information being transferred, the data controller will need to consider other legislation, any risks this may pose, the likelihood of the controller or the processor being subject to that legislation and how the controller will respond if necessary. The data controller should have procedures and measures in place to deal with any requests for information they or their processor may receive under legislation in the country in which the processor is located.

5.12 If either the data controller or the data processor receives a request for information from another jurisdiction, the data controller will need to decide whether or not they are able to comply with the request. If they do decide to comply, then it is good practice to ask for more information if necessary, to make sure the request is specific enough to allow them to be able to identify, retrieve and transfer only that information that is relevant and necessary to comply with the request.