
NOTE ON EXPORTING PERSONAL DATA FROM THE UNITED KINGDOM



KEMP LITTLE LLP

NOTE ON EXPORTING PERSONAL DATA FROM THE UNITED KINGDOM

TABLE OF CONTENTS

A. INTRODUCTION	3
B. THE LEGISLATIVE CONTEXT.....	3
1. EC Data Protection Directive	3
2. The Data Protection Act 1998	3
3. Relevant Definitions	4
C. IN PRACTICE.....	4
1. Commissioner’s Perspective.....	4
2. ‘Good Practice Approach’	5
3. Common Practice.....	5
D. NATURE OF EXPORT	6
1. Transfer or Transit	6
2. Variation of Data Status.....	6
3. Creation of Websites.....	7
E. ADEQUACY OF PROTECTION	7
1. Adequacy in Third Countries.....	7
2. Findings of Adequacy	7
3. Adequacy in United States of America.....	7
4. Evaluating Adequacy	9
5. General Adequacy Criteria	10
6. Legal Adequacy Criteria.....	10
F. ALTERNATIVE MEANS OF ACHIEVING ADEQUACY OF PROTECTION	11
G. MODEL CONTRACTUAL CLAUSES	12
1. Concept.....	12
2. Data Exporter Clauses	13
3. Data Processor Clauses.....	13
4. New Model Clauses.....	14
5. Amendment and Variation.....	15
H. BINDING CORPORATE RULES.....	16
1. Concept.....	16
2. Process	16
3. Multiple Points of Export	17
I. OTHER EXEMPTIONS	18
1. Nature of Other Exemptions	18
2. Consent.....	19
3. Freely Given	19
4. Specific and Informed.....	20
5. Performance of Contract.....	21
6. Legal and Emergency Requirements	21
J. ENFORCEMENT OF COMPLIANCE	22
1. Enforcement by Commissioner	22
2. Criminal Penalties.....	22
3. Civil Proceedings.....	22

NOTE ON EXPORTING PERSONAL DATA FROM THE UNITED KINGDOM¹

A. INTRODUCTION

Increasingly, United Kingdom (“UK”) based controllers of individuals’ data are using third parties in other countries to carry out data processing on their behalf. Whether this is driven by the need for a UK data controller to operate within a multinational corporate structure or simply seeking to take some benefit from the undeniable globalisation of trade through outsourcing customer and employee facing business functions, is irrelevant for the purposes of regulation.

Once a data controlling organisation seeks to export personal data out of defined European territories it becomes subject to substantial legal controls on how that export might be achieved. This note considers the impact of UK and European data protection legislation on exports of personal data between the UK and countries outside the European Economic Area and focuses on:

- the legislative context and application of that law in practice – **Sections B and C**;
- the nature of data exports which are regulated – **Section D**;
- the level of protection deemed adequate for exported personal data– **Section E**;
- the means by which adequate protection might be achieved– **Section F to H**;
- the situations which are exempted from such considerations of adequacy– **Section I**; and
- the means by which compliance with the pertinent legislation is brought about– **Section J**.

B. THE LEGISLATIVE CONTEXT

1. EC Data Protection Directive.

Article 25(1) of the EC Data Protection Directive (the “**Directive**”)², requires EU member states to provide that:

- transfers of personal data
- to a third country
- where the transfer is itself a processing of that personal data or it is intended to process the personal data subsequent to the transfer

may occur (subject to limited exceptions) only if the relevant third country ensures an **adequate level of protection** for the personal data.

2. The Data Protection Act 1998.

¹ Calum Murray, Partner, Kemp Little LLP, London. This note is not legal advice or a substitute for it.

² Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L281/31) – see http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

The eighth and final data protection principle (the “**Eighth Principle**”) of the UK legislation implementing the Directive, the Data Protection Act 1998 (the “**DP Act**”)³, replicates the requirements of Article 25(1) by setting out:

“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.”⁴

3. **Relevant Definitions.**

Any consideration of the effect of the Eighth Principle requires an understanding of the underlying defined terms of the DP Act⁵ which set out:

- a “**data controller**” is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;
- a “**data processor**”, in relation to personal data, is any person (other than an employee of the data controller) who processes the data on behalf of the data controller;
- a “**data subject**” is an individual who is the subject of personal data;
- “**personal data**” is data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller; and
- “**processing**”, in relation to data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.

Throughout this note where the above terms are used it is intended to refer to those terms as defined in the DP Act. Lastly, with regard to the territorial scope and effect of the Eighth Principle, the European Economic Area (the ‘**EEA**’) consists of all EU Member States along with Iceland, Liechtenstein and Norway. Consequently all other countries are regarded as “**third countries**” for the purposes of the DP Act and the Eighth Principle as they give effect to the Directive. All transfers of personal data by a data controller within the UK to a recipient outside the EEA are subject to compliance by the data controller with the Eighth Principle.

C. **IN PRACTICE**

1. **Commissioner’s Perspective.**

In considering how to undertake any exports of personal data from the United Kingdom to a third country, data controllers must consider not only the terms of the DP Act in respect of such transfers but also the UK Information Commissioner’s (the “**Commissioner**”) published guidance

³ see http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

⁴ paragraph 8, Part I, Schedule 1, DP Act – see http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9

⁵ set out in section 1(1), DP Act – see http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_2#pt1-11g1

(the “**Guidance**”)⁶. This additional obligation is evident from the approach adopted by the Commissioner who has stated that if required to examine any data 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 [the Guidance]”⁷.

Given his stated approach on transfers under the Eighth Principle, as a starting point the Commissioner proposes that data controllers should consider all means of achieving their desired ends without processing personal data. The Commissioner gives the example of anonymised data which as it does not relate to identifiable individuals is not personal data, so its processing is beyond the realm of the DP Act. This in turn means any transfer of such anonymised data could be made freely.

2. ‘**Good Practice Approach**’ .

Data Controllers will not always be in a position to find an alternative to data transfers which may be subject to the regime of the Eighth Principle. In such instances the Commissioner has advised data controllers to follow a four-step "good-practice approach" to assess compliance of the data transfer with the DP Act as follows:

- **1.** will the data controller transfer personal data to a third country? – see **Section D** below.
- **2.** does the third country and the circumstances surrounding the transfer ensure that an adequate level of protection will be given to that data - see **Section E** below.
- **3.** are there adequate safeguards to protect the data - see **Section F, G and H** below.
- **4.** will an exemption to the Eighth Principle apply to the transfer - See **Section I** below.

This ‘good practice approach’ has the Commissioner encouraging data controllers to assess the adequacy of the protection afforded to the transferred data in the destination country before making any transfer. The Commissioner is keen that data controllers should not simply rely on one of the exemptions set out in the Act.

3. **Common Practice.**

Given that each such assessment requires a complex combination of :

- an evaluation of a various general adequacy criteria; and
- a legal analysis of the data protection legislation in force in the destination country

data controllers are reluctant to attempt this assessment when reliance can be placed on pre-vetted and simpler methods of compliance with the requirements of the Eighth Principle. This leads many data controllers to:

⁶ “*The Eighth Data Protection Principle and international data transfers - The Information Commissioner’s legal analysis and recommended approach to assessing adequacy including consideration of the issue of contractual solutions, binding corporate rules and Safe Harbor.*” Version 2.0 dated 30.06.06 - see http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/international_transfers_legal_guidance_v2.0_300606.pdf

⁷ See note 6 ante at A1.4

- rely on a EC finding of adequacy;
- employ mechanisms, such as:
 - model contract clauses for transfers between parties; and
 - binding corporate rules for transfers between members of the same group of companies;
- look for the cover of one of the exemptions in Schedule 4 of the DP Act.

These are considered in turn below.

D. NATURE OF EXPORT

1. Transfer or Transit.

In evaluating the need to comply with the Eighth Principle data controllers within the UK must first have regard to the nature of the export of personal data which they are to undertake. This corresponds with step 1 of the Commissioner’s ‘good practice approach’⁸. If the export results in a transfer where the destination is outside of the EEA, and so a third country, then the export must be done in accordance with the Eighth Principle. This should be compared with a situation where personal data is routed through a third country – perhaps on a telecommunications network or similar – but there is no processing of the personal data whilst in that third country and the personal data has an ultimate destination within the EEA. In such circumstances the export need not be carried out in line with the Eighth Principle.

This understanding is confirmed by the Commissioner. In his Guidance the Commissioner states that⁹:

“[the DP 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”

Consequently exports which result in such ‘transitory’ routing through third countries are not subject to the requirements of the Eighth Principle.

2. Variation of Data Status.

Where parties in the UK hold data which is not personal data and intend to export that data from the EEA for processing which would render the data to be personal data subject to the DP Act were it not for the export, they are expected to treat the transfer of that data as being within the scope of the requirements of the Eighth Principle. The Commissioner has suggested that such a situation would arise where data is exported by someone in the UK over the telephone to someone in a third country who then creates a database entry of that data through a computer¹⁰.

⁸ as described in Section C2 above

⁹ see note 6 ante at 1.3.2

¹⁰ see note 6 ante at 1.3.3.

3. **Creation of Websites.**

As social networking websites proliferate and the publication of personal information on websites is ever more common, defining the impact of the Eighth Principle on such website use is necessary. This matter has been addressed by the European Court of Justice¹¹ who opined that:

- there is no transfer of personal data to a third country where an individual loads personal data in an EU Member State onto a website using a internet hosting provider in that Member State even if the website can be accessed by users in a third country; but
- a transfer of personal data does take place where the relevant page is actually accessed by the user located in the third country.

From this judgement, simply uploading personal data onto websites hosted in the EU is not a transfer for the purposes of the Eighth Principle. The reality of the use of websites for personal and business purposes is that there is very often the intention that the data be accessed in a third country – this is the flexibility which the internet brings to communications and the benefit many users seek to enjoy. This means that there will commonly be transfers and the Eighth Principle will apply each time the relevant personal data is viewed by users outside the EEA.

E. ADEQUACY OF PROTECTION

1. **Adequacy in Third Countries.**

Having completed step 1 of the Commissioner’s ‘good practice approach’, if the outcome is that a data controller recognises its processing of personal data will involve an export to a third country, the data controller must settle on whether the third country ensures an adequate level of protection, or ‘adequacy’, for that personal data. The data controller may rely on an EC finding of adequacy or undertake its own adequacy test.

2. **Findings of Adequacy.**

Both the Directive and the DP Act require that, where the European Commission (the ‘**Commission**’) has made a finding that a third country does, or does not, ensure adequacy, that finding shall determine any question as to whether there is adequacy for personal data transfers to the third country by data controllers in the EEA.¹²

As at time of publication, the Commission has made positive findings of adequacy in relation to Argentina, Canada (for recipients subject to the Canadian Personal Information Protection and Electronic Documents Act), Switzerland, the Isle of Man and Guernsey. The Commission publishes its list of “adequate” destinations for data exports.¹³

3. **Adequacy in the United States of America.**

¹¹ In the case of *Bodil Lindqvist v Kammaraklagaren* (2003) (Case C- 101/01).

¹² Article 25(6) of the Directive and paragraph 15, Part II, Schedule 1 of the DP Act- see http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9

¹³ For an up-to-date list of ‘adequacy’ findings see - http://europa.eu.int/comm/justice_home/fsj/privacy/thirdcountries/index_en.htm

The United States of America (“US”) is not generally considered by the Commission to offer an adequate level of protection for transfers of personal data. It is however possible for UK based data controllers to export personal data to US based entities if the recipient entity has signed up to the ‘**Safe Harbor Agreement**’¹⁴. This Agreement was established by the Commission and the US government and has been operational since 1 November 2000. US entities which subscribe to the Agreement are listed on the US Department of Commerce website and there have been almost 1500 to date¹⁵. Those entities are required to operate as regards privacy in line with certain principles (the “**Safe Harbor Principles**”), which have been approved by the Commission and are administered by the US Department of Commerce. The Safe Harbor Principles reflect much of the principle behind the Directive and the privacy regime it creates. In particular the Safe Harbor Principles require:

- *Notice* - individuals must know what information is collected, what will be done with it (including third party sharing) and how to contact the entity with enquiries or complaints;
- *Choice* - individuals must have the opportunity to opt out of any use or disclosure of their personal information and for sensitive information, opt in choice must be given if the information is to be disclosed to a third party or used for additional purposes;
- *Onward Transfer* - for transfers to third parties, entities must apply the notice and choice principles;
- *Access* – generally individuals must have access to personal information held about them and be able to correct, amend, or delete that information where it is inaccurate;
- *Security* – entities must take reasonable precautions to protect personal information from loss, misuse and unauthorised access, disclosure, alteration and destruction;
- *Data integrity* - personal information must be relevant for the purposes for which it gathered and be kept accurate, complete, and current; and
- *Enforcement* - readily available and affordable independent recourse mechanisms for complaint investigation resolution and compensation; procedures for verifying adherence to the Safe Harbor Principles; and obligations to remedy problems arising out of a failure to comply with the Safe Harbor Principles.

Once a US entity has signed up to the Safe Harbor Agreement it is authorised to accept data transfers from the EU without the need for data subject approval or additional compliance with other legal or regulatory requirements. Should a signatory breach the Safe Harbor Principles, both the US Federal Trade Commission and the injured data subjects may raise actions against the entity under the applicable adjudication scheme from which the entity has accepted jurisdiction in line with the ‘enforcement’ Safe Harbor Principle. It should be noted that the regime provided by the Safe Harbor Principles does not apply to all business sectors and entities active in telecommunications and financial institutions are likely to fall outside of this means of showing adequacy. In respect of the transfer of personal data to such industries, as with US entities which

¹⁴ For full details of Safe Harbor, the Agreement and the Safe Harbor principles – see <http://www.export.gov/safeharbor/>

¹⁵ see <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>

have not signed up to the Safe Harbor Agreement these transfers are to be considered like any other export from the UK to a third country.

4. Evaluating Adequacy.

For exports of personal data to a third country which have not been subject to a Commission finding of adequacy, UK data controllers are obliged to assess adequacy in line with the Directive and the Act. In practice such evaluations are rare with data controllers instead preferring to rely on other means of establishing adequate protection be it:

- contractually – through model clauses;
- organisationally – using binding corporate rules; or
- legally - relying on the exemptions to the need for adequacy which are set out in Schedule 4 of the DP Act.

These means are considered further in **Sections F to I** below.

Circumstances may arise where the assessment by the data controller cannot be avoided. If so it should be noted that in carrying out an assessment of adequacy, the Commissioner, as set out in the Guidance, expects exporting data controllers to be able to demonstrate how they have addressed the various evaluation criteria¹⁶. Consequently UK data controllers will have to consider all the evaluation criteria of the DP Act¹⁷ which are derived from Article 25(2) of the Directive. To be adequate, the level of protection afforded to personal data in the third country must be “adequate in all the circumstances of the case”¹⁸ with particular consideration given to certain criteria. In the Guidance¹⁹, the Commissioner divides these criteria into the:

- ‘general adequacy criteria’
 - 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;
 - the country of final destination of the personal data; and
- ‘legal adequacy criteria’
 - 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.

¹⁶ see note 6 ante at 2.3.1

¹⁷ paragraph 13, Part II, Schedule 1, DP Act - see http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9

¹⁸ *ibid*

¹⁹ see note 6 ante at 2.3.4

5. General Adequacy Criteria.

The Commissioner believes that the exporting data controller will be able to identify easily general adequacy criteria and as such the general adequacy criteria should be assessed by the controller for each export. This will require the exporting data controller to consider:-

- *the nature of the personal data* – transfers of little risk to data subjects' rights are not likely to require the higher level of protection which would be inherent when exporting sensitive personal data;
- *the purpose(s) of the proposed transfer* - some purposes will carry a lesser risk to data subjects' rights than others, for example where the purpose is a one-off or the passing of limited information such as contact details;
- *the period during which the data are intended to be processed* –as with the one-off use above there is naturally a greater risk to personal data if it is kept for a longer period of time. In line with the general requirements of the DP Act personal data should be deleted by the data recipient once no longer required for the intended purpose;
- *any security measures taken in respect of the data in the third country* – by requiring organisational and technical security measures preventing unauthorised access to the personal data the adequacy of the protection is enhanced. Use of encryption or the adoption of standardised information security management practices (akin to ISO17799/BS7799) assist data security;
- *the country of origin of the personal data* – if the personal data was originally gathered in a third country, the level of protection expected in that country is relevant when considering adequacy as this will establish the data subject's expectation as to what protection his personal data should enjoy. The Commissioner has confirmed that the DP Act is not intended to provide greater protection to an individual in a third country than he has under the data protection regime of that third country; and
- *the country of final destination of the personal data* - if UK data exporter is aware prior to exporting that the recipient of the data will also transfer the personal data to a third country, he must consider the adequacy of the protection of the final destination. In such arrangements the exporting data controller would be recommended to contractually oblige the data recipient to which it is exporting not to further transfer the personal data unless the further transfer complies with all applicable UK data protection laws.

6. Legal Adequacy Criteria.

The Commissioner acknowledges that legal adequacy criteria of:

- 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,

may be more difficult for the data controller to assess as an exhaustive analysis of the legal system in force in the third country may be impossible²⁰. The Commissioner recommends that the outcome of an assessment of the general adequacy criteria can assist data controllers in deciding the level of legal adequacy analysis to undertake. If the general adequacy has revealed that in the particular circumstances the transfer is high risk then a more comprehensive investigation of the legal adequacy criteria will be expected.

In addition the Commissioner believes it is reasonable for an analysis of the legal adequacy criteria to be carried out by the data controller when the exporting of data to the third country is likely to be a common occurrence should the data controller be proposing to set up a permanent operation in the third country.

Lastly even if a data controller fails to conduct a full analysis of the legal adequacy criteria, the Commissioner expects data controllers to be able to identify third countries posing a danger of prejudice at the time of the transfer because of, for example, instability in the third country and act with suitable caution in respect of such transfers.

F. ALTERNATIVE MEANS OF ACHIEVING ADEQUACY OF PROTECTION

As set out in Section E adequacy of protection for a personal data export from the EEA can be established by the:

- Commission through a blanket finding of adequacy;
- Commission and a third country government through agreement; and
- data controller through general and legal adequacy evaluations.

Where the Commission has not so acted; a data controller cannot undertake an adequacy evaluation; or where the outcome of the adequacy assessment by the data controller finds inadequate protection for the personal data, alternative means of ensuring adequate protection must be found. This ties to the third step of the Commissioner's good practice approach, namely, ensuring adequate safeguards to protect the exporting personal data.

Article 26(2) of the Directive 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..."

And this in turn is implemented by paragraphs 8 and 9 of Schedule 4 to the DP Act. From this it is open to the Commissioner under Article 26(4) to recognise standard contractual clauses as offering adequate safeguards for the purposes of Article 26(2). In turn this allows data controllers to use such contractual terms to ensure protection is present at an adequate level. This can be achieved through the use of Commission authorised model contract clauses (see **Section G**

²⁰ see note 6 ante at 2.5

below) or specific, approved binding corporate rules (“**BCR**”) (see **Section H** below). Transfers which are made in either of these ways are made exempt from the regime of the Eighth Principle as the model contract clauses or BCRs are themselves adequate safeguards for data subjects’ rights. It is also open to the Commissioner to provide individual authorisations of data exports under Articles 26(2) and (4) but those powers are likely to be exercised in exceptional circumstances only.

It should be noted that transfers exempted from the regime of the Eighth Principle through Article 26(2) must ensure conditions for the relevant data subjects to continue to be protected as regards processing of their data even after the data have been transferred. As such the Commissioner has stated²¹ it is good practice to attempt to satisfy one of these Article 26(2) derogations before considering the exemptions which derive from Article 26(1) as implemented in paragraphs 1 to 7 of Schedule 4 to the DP Act (for a discussion of the latter exemptions see **Section I** below).

G. MODEL CONTRACTUAL CLAUSES

1. Concept.

As noted in **Section F**, the Commission is empowered by Articles 26(2) and (4) of the Directive to decide that certain standard contractual clauses offer adequate safeguards for the protection of personal data and data subjects’ rights. Under the terms of such an agreement the recipient must provide adequate safeguards in respect of the personal data. The Commission has approved three sets of model contractual clauses (“**Model Clauses**”) which Member States must recognise as ensuring adequacy. These are set out as an annex to the relevant Commission decision which approves them:

- the first set is for use by EU-based data controllers when transferring personal data to **data controllers** outside the EEA (“**Data Exporter Clauses**”)²²;
- the second set is for use by EU-based data controllers when transferring personal data to **data processors** outside the EEA²³ (“**Data Processor Clauses**”); and
- the third set, like the first set, is for use by EU-based data controllers when transferring personal data to **data controllers** outside the EEA²⁴ (“**New Model Clauses**”).

Use of the Model Clauses is accepted as adequate by all data protection regulators throughout the EU. In the UK the Commissioner has issued authorisations under s54(6) of the DP Act in relation to each of the Model Clauses 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

²¹ see note 6 ante at 3.1.2

²² Commission Decision 2001/497/EC15 of 15 June 2001 – see http://eur-lex.europa.eu/pri/en/oj/dat/2001/l_181/l_18120010704en00190031.pdf

²³ Commission Decision 2002/16/EC16 of 27 December 2001 – see http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_006/l_00620020110en00520062.pdf

²⁴ Commission Decision 2004/915/EC17 of 27 December 2004 – see http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00740084.pdf

Clauses. As a consequence of this, one of the options for a data controller seeking to export personal data from the UK to a third country outside the EEA is for it to enter into a data transfer agreement with the recipient of the data. It should be noted that in certain Member States, though not the UK, it is necessary to file a copy of the Model Clauses as agreed between the parties with the relevant data protection regulator before an export of personal data can be undertaken. It should also be noted that the Commission does not allow the parties to vary the Model Clauses on substantive issues.

The terms of the Model Clauses vary depending on the relationship between the contracting parties and the set used.

2. Data Exporter Clauses.

The Data Exporter Clauses have the following central elements:

- the data exporter must ensure that all pre-transfer personal data processing is in accordance with the DP Act and other applicable law;
- the data importer may process the personal data only in accordance with applicable law and the mandatory principles relating to transparency, data quality and proportionality, security and confidentiality as set out in the Data Controller Clauses (and replicating the Directive);
- the data importer must submit its data protection facilities for audit by the data exporter or as may be required by a relevant data protection regulators;
- the data exporter and the data importer are jointly and severally liable for any breach which results in a data subject suffering damages unless both data exporter and data importer can prove that neither of them is responsible for the breach; and
- all relevant data subjects are third party beneficiaries who can enforce the Data Exporter Clauses.

The issue of joint and several liabilities has been the most contentious in relation to the use of the Data Exporter Clauses and has led to parties looking for other means of achieving adequacy and ultimately the New Model Clauses. Under the Data Exporter Clauses, nothing can be done to avoid joint and several liability, regardless of the diligence of the data exporter or the negligence of the data importer. As discussed in **Section G4** below, this is largely addressed in the New Model Clauses.

3. Data Processor Clauses.

Where the data transfer is between a data controller and a data processor, the data transfer requires a different level of control as the data controller is deemed by law to remain in control of, and responsible for, the personal data. The Data Processor Clauses have the following central elements:

- the data controller must ensure that all pre-transfer personal data processing is in accordance with the DP Act and other applicable law;
- the data controller must provide instructions to the data processor on processing the personal data;

- the data controller must ensure that the data importer has put in place adequate technical and organisational measures to protect the personal data;
- the data processor may process the personal data only in accordance with applicable law and instructions of the data controller;
- the data processor must put in place adequate technical and organisational security measures to protect the personal data; and
- the data controller is liable for any breach (even if the breach was caused by the data processor) which results in a data subject suffering damages save where the data controller becomes bankrupt, has disappeared or ceased to exist, when the data importer assumes full liability.

The Data Processor Clauses also address the requirements imposed on data processors by the seventh data protection principle, namely that the data controller ensures that appropriate technical and organisational measures are taken at all times against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.²⁵

Use of the standard clauses is not mandatory and the data controller may ensure compliance with the seventh and Eighth Principles by other means, but using the Data Processor Clauses is a simple way of ensuring such compliance.

4. New Model Clauses.

As set out in **Section G2** above, the Data Exporter Clauses were not met with widespread acclaim, particularly due to their liability regime. Consequently and following requests for the less onerous Model Clauses, the Commission added a new set of standard contractual clauses in the New Model Clauses. The New Model Clauses apply only to transfers from one data controller to another and not to transfers of personal data between data controllers and data processors. This now affords data exporters a choice of Model Clauses to use in their data controller to data controller arrangements. It should be noted that it is not permissible to amend the New Model Clauses nor combine them with the Data Exporter Clauses. Unlike the Data Exporter Clauses, the New Model Clauses contain 4 ‘commercial’ clauses the use of which is optional.

In respect of liability, the New Model Clauses require each data controller to be responsible for its own breach. In line with this several liability, data subjects (who maintain their rights as third party beneficiaries under the New Model Clauses) may only enforce the New Model Clauses against the data controller who has committed the breach. Any such action must be brought in the exporting data controller's jurisdiction of establishment.

A trade-off for the data exporter's reduction of potential liability is present in the New Model Clauses, in that the data exporter assumes a greater responsibility for resolving data subjects' complaints. Should a data subject allege a violation of the data subject's rights by the data importer, the data subject must ask the data exporter to enforce the data subject's rights against

²⁵ paragraph 7, Part I, Schedule 1, DP Act - see

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9

the data importer. If such action is not taken within a reasonable period of time (set at one month in the New Model Clauses), the data subject can enforce his rights directly against the data importer. Furthermore if the data subject can establish that the data exporter failed to use reasonable efforts to check that the data importer could comply with its obligations under the New Model Clauses, the data subject can take direct action against the data exporter.

The combined effect of the changes in the New Model Clauses is to present a more attractive route to data controller to data controller data exports. However, as the Commission made clear when introducing the New Model Clauses:

“to prevent abuses with this additional flexibility...data protection authorities can more easily prohibit or suspend data transfers based on [the New 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”²⁶

so there is an increased chance that a data protection regulator may intervene under the New Model Clauses if breach of those clauses occurs. This should be contrasted with the Data Exporter Clauses, under which data protection regulator can only suspend a data flow when there is evidence that the continuation of the transfer would create an imminent risk of great harm to a data subject.

5. Amendment and Variation.

As set out in **Section G1** above no version of the Model Clauses may be amended by the parties if they are to enjoy the finding of providing adequacy for the purposes of the Eighth Principle. Data exporters may include any other clauses on business related issues where they do not contradict the Model Clauses and, in turn, the Model Clauses may be incorporated into data exporters’ wider agreements. Furthermore, the New Model Clauses allow parties to update the description of the data transfer which the parties have originally contracted for to reflect changes as their relationship develops.

Should a data exporter use any of the versions of the Model Clauses, be it stand-alone or incorporated into another contract, and make changes to the wording of any clause (but not its intended meaning or effect) this new wording does **not** amount to use that is authorised by the Commissioner under paragraph 9 of Schedule 4 to the DP Act²⁷. However, this does not prevent the data exporter from evaluating that the data export is made on terms which provide adequacy as discussed in Section E above. The Commissioner has stated that use of different terms with the same meaning or effect as those in the Model Clauses will be a significant factor if the Commissioner is required to assess the adequacy of any protection given to data exported under such terms²⁸.

Lastly, it is the Commissioner’s view that if the only change to the Model Clauses is to make the contract between more than two parties rather than remain a bilateral agreement between one data exporter and importer then this does remain within the scope of the Commissioner’s authorisation provided that the obligations of all the parties remain clear and legally binding²⁹.

²⁶ see note 24 ante at paragraph 7

²⁷ see note 6 ante at 3.2.6

²⁸ *ibid*

²⁹ see note 6 ante at 3.2.7

H. BINDING CORPORATE RULES

1. Concept.

Exporting personal data outside the EEA in a legally compliant manner can be achieved by corporate data controllers through the use of Model Contractual Clauses as set out in **Section G** above. However, it is unlikely that Model Contractual Clauses will form a sufficiently robust solution for businesses which: operate in multiple countries; have many subsidiaries; and/or which transfer a variety of personal data for different purposes. The concept of using Binding Corporate Rules (“**BCR**”) to create adequate safeguards for the purposes of Article 26(2) was established by the Working Party³⁰. BCR are legally enforceable (by data subjects) intra-multinational corporate group internal codes of conduct, approved by the Commissioner, adherence to which by UK companies and their non-EEA corporate group companies means transfers of personal data will comply with the Eighth Principle. Essentially the BCR are a further way of protecting data subjects’ rights and ensuring adequacy for transfers of personal data to third countries. A key benefit of BCR are that they can be prepared to meet the needs of the relevant multinational organisation rather than the organisation having to fit its practices around more rigid terms such as the Model Contractual Clauses.

2. Process.

To make intra-group data exports from the UK to third countries on the basis of the BCR, the BCR must first be submitted for approval by the Commissioner in order to obtain an authorisation. The Working Party has developed a model checklist on the content of a BCR application³¹; a co-operation procedure which explains how to submit BCR for approval by the data protection authorities and how they will cooperate to come to a common opinion on the BCR³²; and a standard application form based on the model checklist³³. Use of the standard application is not mandated in the UK, however given its basis on the model checklist, in using it applicants are assured that they will address the necessary requirements of the checklist.

Applicants to the Commissioner for the authorisation of BCR are required to demonstrate their application is in accordance with the model checklist and how the required adequate safeguards are in place within the organization. There is no pre set form for the structure or content of BCR. It is more important that the substance of the BCR is comprehensive around the requirements of the model checklist, such as:

³⁰ in its working document on binding corporate rules, “*Working Document (WP74) 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 (‘**WP74**’) 3 June 2003 - see

http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf

³¹ “*Working Document (WP108) Establishing a Model Checklist Application for Approval of Binding Corporate Rules 05/EN WP108*” 14 April 2005 (‘**WP108**’) – see

http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf

³² “*Working Document (WP107) Setting forth a co-operation procedure for issuing common opinions on adequate safeguards resulting from binding corporate rules 05/EN WP107*” (‘**WP107**’) 14 April 2005 – see http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp107_en.pdf

³³ “*Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*” 10 January 2007 (‘**WP133**’) - see

- http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp133_en.doc

- *evidence that the measures are binding, both internally and externally* – BCR must be legally enforceable and this requires evidence that, under applicable law, the BCR are binding on all intra-group companies, be it contractually, through one group company having the legal power to bind its affiliates, or a unilateral undertaking given by the parent company;
- *evidence that the measures are enforceable by the data subjects* – it is necessary that the BCR can be enforced by the data subjects as third party beneficiaries. A data subject must be able to start an action: (i) within the exporting Member State; (ii) against the EU headquarters of the group; and (iii) against the group member delegated data protection responsibilities under the BCR. Applicants for BCR must display that the delegated group member is able to pay compensation for any damages resulting from a breach of the BCR.
- *details of a data protection audit plan* – setting out how compliance with the BCR will be monitored in the group through an audit plan and programme;
- *nature of the data processing and flows of information* – a full description of all processing purposes, and transfer destinations to allow fully informed evaluation of adequacy;
- *description of the data protection safeguards in place* - BCR must describe how the requirements of the Directive for data protection safeguards will be achieved by the safeguards it puts in place;
- *details of sub-contracting terms* – setting out the how contractual clauses will be imposed on sub-contractors used for data processing, and what sanctions will flow from a breach of those conditions; and
- *details of a mechanism for reporting and recording changes and complaints* – BCR must explain how changes will be communicated intra-group and to the Commissioner and also how data subjects' complaints can be dealt with adequately, efficiently and effectively.

The Commissioner has stated in his Guidance that he will only give an authorisation where he is satisfied that adequate safeguards can be delivered.

BCR applications must be submitted for approval by one company from the corporate group. If the ultimate parent or operational headquarters of the group is incorporated in a Member State, that Company should file the application. Where the ultimate parent is not located in a Member State, an EU established company should be appointed as the responsible party for the BCR.

3. Multiple Points of Export.

Where a data controlling organisation is going to the effort of introducing BCR it is unlikely that it will only be seeking to export data from the UK to a third country, it being more likely that the company will have multi-EU operations from each of which it plans to make data exports. In such circumstances WP 74³⁴ provides a mechanism for the exporting data controller to liaise with

³⁴ see note 22 ante.

a data protection regulator who then co-ordinates the authorisation process in all the other European jurisdictions in which that company is data controller.

The selection of the lead data protection regulator must be justified in the application for approval of the BCR³⁵. The following criteria are stated by the co-operation procedure³⁶ to be relevant in the selection of the lead DPA, namely the location:

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

with the location of the group's European headquarters commonly the deciding factor. It is, however, open to the relevant data protection regulators to decide to allocate the lead data protection regulator to another Data Protection Authority than the one proposed by the applicant.

If Companies transfer data from more than one Member State, they will still have to comply with any additional national requirements of such Member States, such as notification or administrative formalities. Once a set of BCR have been approved, and any necessary local regulations been complied with, any exports falling within their scope can take place from the countries from which authorisations have been received. While transfers made under intra-group codes not submitted for the Commissioner's approval by 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 (See **Section E**). The Commissioner's website contains further information as to how to make an application for the authorisation of BCR³⁷.

I. OTHER EXEMPTIONS

1. Nature of Other Exemptions.

Article 26(1) of the Directive³⁸ provides a set of limited exemptions which allow the transfer of personal data to a third country even if that third country does not provide an adequate level of protection for personal data as otherwise required under the Directive. These exemptions are reflected in Schedule 4 of the DP Act³⁹ as limited circumstances where the Eighth Principle does not apply. The rationale behind these exemptions is that there are instances where it will be justifiable to transfer personal data even though there will be a lower level of protection given to

³⁵ see WP 107 and WP 108, notes 23 and 24 ante respectively

³⁶ see note 24 ante.

³⁷ see - <http://www.ico.gov.uk/eventual.aspx?id=1163#Binding%20Corporate%20Rules>

³⁸ see note 2 ante at Article 26(1)

³⁹ Schedule 4, DP Act – see http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_11

those data. These justifications are generally founded on grounds of free choice of individuals or over-reaching interest which necessitates the transfer.

In his Guidance, the Commissioner considers that data controllers as a matter of good practice should ensure that there is adequate protection for personal data they are exporting, instead of merely sheltering under an exemption to the Eighth Principle. Despite there being exemptions to the requirements the Commissioner recommends that, in interpreting the exempting provisions, a narrow construction should be taken⁴⁰. The exemptions most commonly relied on are considered further below.

2. **Consent.**

Data controllers may export personal data to a third country which does not provide an adequate level of protection for that personal data if the data subject provides their unambiguous consent to that export⁴¹.

As with processing personal data generally, reliance on consent as a ground for exporting such personal data must overcome the absence of a definition of "consent" in the DP Act. While the term has not been clarified in the UK legislation, the Directive defines consent as:

*"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"*⁴²

The Article 29 Working Party of national regulators was set up under Article 29 of the Directive ("**Working Party**"). It is an independent European advisory body on data protection and privacy in terms of Article 30 of the Directive. As part of a project to produce a working document on a common interpretation and application of the exemptions set out in Article 26 of the Directive the definition of consent in that Article has been further considered by the Working Party.⁴³

Whilst not carrying the weight of law, the opinions of the Working Party have direct impact on practice of regulators across EU Member States, such as the Commissioner. Following the Working Party's working document, the Commissioner has confirmed that obtaining consent is not a simple matter. There are several elements which must be present in the consent.

3. **Freely Given.**

To ensure that consent is 'freely given' the data subject must not be co-erced into providing the consent, nor should that consent be derived from a situation where the data subject believes they have no choice in the matter of giving consent or where failure to so consent might result in the data subject suffering a penalty.

⁴⁰ see note 6 ante at 4.1.2

⁴¹ see note 2 at Article 26(1)(a)

⁴² see note 2 ante at Article 2(h)

⁴³ Working document 2093/05/EN – WP114 - see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf

The Commissioner's Guidance suggests that exporting controllers should be able to produce evidence of the data subject's consent in any particular case and may be required to demonstrate that the data subject was fully informed regarding the transfer as required.⁴⁴

In practice this leads to data controllers obtaining consent through a process of notification of the data controller's intentions for the data prior to individuals submitting data and the provision of a means of recordable consent. This is commonly achieved manually through ticks on paper forms or clicks electronically by a similar process online. It should be noted that the Directive does not require such consent to be in writing, electronic or manuscript. Use of writing in this way is, however, a simple and if done correctly, effective means of the data controller being able to show all necessary consents have been properly obtained.

4. **Specific and Informed.**

In addition to consent being freely given, it is essential that the consent is specific to the processing purposes which the data controller has set out in its notification to the data subject. It is suggested that as a minimum, data subjects should be notified of the destination, purpose and categories of recipients for the transfer. This in turn will assist in showing that any consent obtained is informed.

Should the data controller successfully implement a means of providing notification and obtaining consent, it must be remembered that the consent will be specific to the circumstances of the processing and transfer notified to the individual. Inherent in this is an inability on the part of the data controller to 'stretch' the consent it has obtained to cover any changes in those circumstances. Additional consent will be required for new transfer conditions which were not present when the original consent was obtained.

In addition to consent being specific, it is not without limit of time. It is always open to data subjects to withdraw their consent to any processing, including exports of data and data controllers are required to act in accordance with the wishes of the individual.

In short reliance can only be placed on the consent exemption where a data subject:

- fully comprehends what transfer is being agreed to;
- is aware of the reasons for the transfer and to as full an extent as possible the third countries to which a transfer will take place;
- has been informed of any specific risks to his personal data involved in the transfer; and
- then consents freely and explicitly to the transfer for so long as that consent remains valid and not withdrawn.

In considering the issue of consent in its working document the Working Party believes consent is:

“unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfers for the processing in question.”⁴⁵

⁴⁴ see note 6 ante at 4.2.1

⁴⁵ see note 14 ante at page 11

Instead of relying on this “*false good solution*”⁴⁶, the Working Party suggest that data controllers look to other derogations from the regime of the Eighth Principle to justify their data exports from the EEA.

5. **Performance of Contract.**

Data controllers may export personal data to a third country which does not provide an adequate level of protection for that personal data if the transfer is necessary to:

- perform a contract with the data subject; or
- take steps at the data subject’s request with a view to entering into a contract with him.

These ‘performance of contract’ exemptions extend to contracts of employment.

In assessing whether this exemption applies, consideration of how “necessary” the transfer is in respect of the contract is central. A transfer will be necessary when the transfer of the personal data is integral to the performance of the contract, such as an online travel portal passing a user’s personal data to a hotel chain when confirming a booking. The Working Party is of the opinion⁴⁷ however that it is an excessive interpretation of the concept of necessity to attempt to avail itself of this exception for a company to claim that the transfer of employees’ data from a subsidiary to a parent company in a third country is necessary when in fact this is a transfer brought about as a result of the preferred operating structure for the parent company. The Working Party believes this lacks a required direct and objective link between performance of an employment contract and such a transfer of data.

6. **Legal and Emergency Requirements.**

Data controllers may export personal data to a third country which does not provide an adequate level of protection for that personal data if the transfer is necessary:

- for reasons of substantial public interest (such as crime prevention or detection) - any transfer of personal data sought to be justified on these grounds should be in the substantial public interest of the Member State which is making the transfer and not the third country to which the transfer is being made. In the UK 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;
- for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), for obtaining legal advice or otherwise for establishing, exercising or defending legal rights – in evaluating whether to rely on this, consideration should again be given to the necessity of the transfer and the need to balance the legal rights in issue with the data subject’s rights in relation to their personal data. It should be noted that the legal proceedings need not involve the data controller or the data subject directly for this exemption to be relied on;

⁴⁶ *ibid*

⁴⁷ *ibid* at page 13

- for the purpose of protecting the vital interests of the individual. The Commissioner considers that this exemption may only be relied upon where the data transfer is necessary for matters of life and death such as a medical emergency⁴⁸.

J. ENFORCEMENT OF COMPLIANCE

1. Enforcement by Commissioner.

Should a data controller breach the Eighth Principle, the Commissioner has the power to issue an enforcement notice. This notice can require the data controller within a set period to either stop the offending data export or comply with the Eighth Principle. Non-compliance with an enforcement notice is a criminal offence⁴⁹. Data controllers in receipt of an enforcement notice have a right of appeal in respect of the notice to the Information Tribunal. Ultimately data controllers may make appeals to the High Court on points of law⁵⁰ from the Information Tribunal. It should be noted that the enforcement strategy previously publicised by the Commissioner is to take a selective approach to enforcing the DP Act, focussing on taking action against breaches of data protection which results in serious consequences.

2. Criminal Penalties .

Those found to have committed criminal offences in relation to the DP Act may face a maximum fine of £5,000 on summary conviction or an unlimited fine if convicted on indictment⁵¹. Company officers may also be liable to prosecution for criminal offences under the DP Act. Where a company commits an offence with the consent of, connivance of, or due to any neglect on the part of, the officer concerned, each of that officer and the company is guilty of the offence.⁵²

3. Civil Proceedings .

A data controller may also face civil proceedings: any data subject suffering damage or damage and distress (but not distress alone) as a result of a data controller's failure to comply with the principles has a right to sue for damages under the DPA (*section 13, DPA*).

**Kemp Little LLP (CGM)
London
April 2008**

⁴⁸ see note 6 ante at 4.6

⁴⁹ set out in section 47, DP Act – see http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_6

⁵⁰ set out in section 49, DP Act – see http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_7

⁵¹ set out in section 60, DP Act – see http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_7

⁵² set out in section 61, DP Act – see http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_7