

**CHAPTER 24  
SECTION 9**

**REQUESTS FROM FOREIGN GOVERNMENTS**

**SECTION CONTENTS**

- 1. [THE DATA PROTECTION ACT 1998](#)**
  - 1.1. [The Eighth Data Protection Principle](#)**
  - 1.2. [Exemptions to the Eighth Principle](#)**
  - 1.3. [Reasons of Substantial Public Interest](#)**
- 2. [REQUESTS FROM WITHIN THE EEA](#)**
- 3. [REQUESTS BY A FOREIGN GOVERNMENT FOR DETAILS OF CONVICTIONS OF ITS NATIONALS](#)**
  - 3.1. [Requests from governments within the EEA](#)**
  - 3.2. [Requests from governments outside the EEA](#)**
  - 3.3. [Proactive disclosures to foreign governments](#)**
- 4. [REQUESTS FOR CERTIFICATES OF CHARACTER](#)**
  - 4.1. [Standard Reply](#)**

## 1. THE DATA PROTECTION ACT 1998

When requested by a foreign government or authority which is outside the European Economic Area to provide personal data about a living individual, in addition to the legal considerations (HRA, DPA, law of confidence, powers) which apply in relation to disclosures to UK public authorities [**see sections 1 and 3 of this IDI**], the eighth data protection principle of the DPA must be considered. Disclosures of personal data to foreign governments are only likely to be lawful under the DPA if necessary for the identification or apprehension of immigration or criminal offenders, for the purpose of legal proceedings, if sanctioned by international agreements such as the Dublin Convention, or with the individual's consent.

### 1.1. The Eighth Data Protection Principle

The eighth Data Protection principle states:

*“Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) 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”*

The EEA consists of the 25 European Union (EU) Member States together with Iceland, Liechtenstein and Norway. It excludes the Channel Islands. The European Commission is empowered to make decisions that particular countries or territories ensure an adequate level of protection for these purposes. So far such decisions have been made in relation to Argentina, Canada, Guernsey, Hungary, Isle of Man, Switzerland, and a set of non-statutory arrangements in the USA known as “safe harbour”.

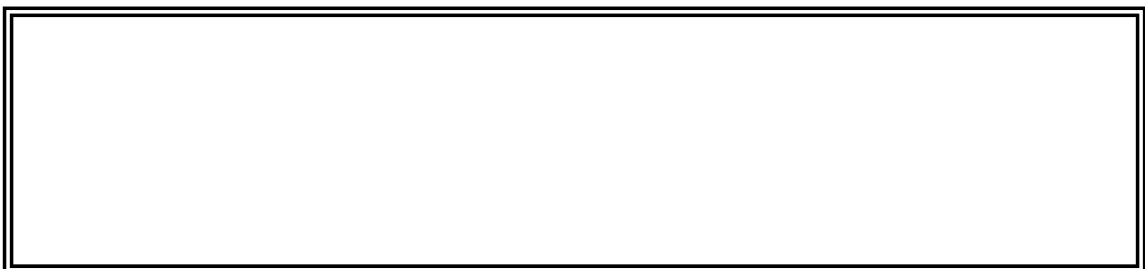
Where no decision has been made in respect of a particular country or territory, and unless an exemption to the eighth principle applies (see below), the UK Border Agency must be satisfied that an adequate level of protection is ensured for these purposes before transferring personal data to the foreign government or authority.

An adequate level of protection is one which is adequate in all the circumstances of the case, having regard to matters such as the nature of the personal data, the country or territory to which the data are to be transferred, the purposes for which and the period during which the data are intended to be processed, the law in force in the country or territory in question, its international obligations, any relevant codes of conduct or other rules which are enforceable there, and any security measures taken in respect of the data there. If it is considered necessary to assess whether a particular country offers an adequate level of data protection, contact the IAPT (0208 760 4657) for advice.

## 1.2. Exemptions to the Eighth Principle

Schedule 4 of the DPA sets out circumstances in which the eighth principle does not apply to a transfer. The circumstances that are most likely to be relevant to the transfer of personal data by the UK Border Agency to a foreign government or authority are:

- The data subject has given their consent to the transfer.
- The transfer is necessary for reasons of substantial public interest (e.g. section 13 of the Immigration and Asylum Act 1999).
- The transfer:-
  - (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
  - (b) is necessary for the purpose of obtaining legal advice, or
  - (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- The transfer is necessary in order to protect the vital interests of the data subject.
- The transfer is made on terms that are of a kind approved by the Information Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects. This is a reference to standard form contracts which the European Commission has published and which must be used in unamended form.
- The transfer has been authorised by the Information Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.



## 1.3. Reasons of Substantial Public Interest.

This exemption to the eighth data protection principle may be relevant in relation to transfers which are necessary for the prevention or investigation of crime, or the detection and identification of immigration offenders. Each case must be considered on its merits and staff should consult with the IAPT if considering such a disclosure.

## 2. REQUESTS FROM WITHIN THE EEA

As mentioned above, the EEA consists of the 25 European Union (EU) Member States together with Iceland, Liechtenstein and Norway. It excludes the Channel Islands.

If a request is received from a country from within the EEA then the eighth principle would not apply and the usual considerations, which apply to disclosures to UK public authorities, would apply [*see section 3*]. All requests for information should be put in writing and the purpose of the disclosure fully explained.

## 3. REQUESTS BY A FOREIGN GOVERNMENT FOR DETAILS OF CONVICTIONS OF ITS NATIONALS

Foreign governments usually make requests for details of criminal convictions of their nationals when that individual is being removed or deported to their country. In some cases the Prison Service will alert the authorities of a country to the fact that one of their nationals has been convicted of a criminal offence and is being returned to that country. The fact that the majority of court cases are open to the public and criminal convictions are a therefore a matter of public record does not mean that disclosure of the details of a conviction to a foreign government is lawful. Staff should follow the guidance below and contact the IAPT if in doubt.

### 3.1. Requests from governments within the EEA

Where the UK Border Agency holds the information which the another government has requested, staff may disclose information about the conviction provided the usual provisions of the DPA and Human Rights Act 1998 (HRA) are met i.e. the disclosure is fair, lawful, necessary and proportionate [*see section 1 of this IDI chapter for further details*].

If the information which the foreign government has requested is not held by the UK Border Agency, staff should refer the requestor to the clerk of the court where the individual was convicted.

### 3.2. Requests from governments outside the EEA

Where the requesting government is from a country outside the EEA, the 8<sup>th</sup> Data Protection principle and the HRA must be borne in mind in addition to the usual DPA and HRA considerations. If disclosure of an individual's criminal history will/may lead to that individual being subjected to treatment which would breach the HRA then that disclosure will be unlawful. Similarly, unless we have the consent of the data subject or disclosure of their criminal conviction to the foreign government is in the substantial public interest disclosure will probably be unlawful.

As mentioned above (in 1.1), some countries outside the EEA have suitable safeguards in place to protect personal data and therefore the 8<sup>th</sup> Data Protection principle will not apply. However, staff must still consider whether the disclosure would breach the HRA prior to disclosing the details of an individual's criminal conviction to one of these countries.

### 3.3. **Proactive disclosures to foreign governments**

Staff may come across individuals being returned or deported to their country of origin and that individual has committed a serious crime in the UK e.g. a paedophile. Where it is clear that the authorities of that individual's country of origin are not aware of the individual's criminal history staff may consider that disclosure of that information is prudent. However, staff must be aware of the need to consider the implications of such a disclosure in terms of the DPA (8<sup>th</sup> principle) and the HRA (see 3.2 above). A disclosure should not be made unless the disclosure is permitted within the provisions of the DPA and HRA. Staff should always seek guidance from the IAPT if considering a proactive disclosure to a foreign government.

## 4. **REQUESTS FOR CERTIFICATES OF CHARACTER**

Certain foreign governments require individual overseas nationals to produce certificates of character before they will issue visas or consider the grant of naturalisation etc. As a general rule the UK Government neither possesses nor wishes to possess information enabling it to certify that a particular individual is of good or bad character for this purpose. Therefore, all requests for certificates of character or criminal records are to be refused.

### 4.1. **Standard Reply**

A standard reply, which may be used in these circumstances, is as follows:

"I am writing in reply to your letter of..... in which you requested a character reference for....."

The UK Border Agency'S records relating to individual overseas nationals do not contain details which would enable me to assess [INSERT NAME OF INDIVIDUAL]'s character. I am afraid therefore that I am unable to provide you with the information that you request."