

SECTION CONTENTS

CHAPTER 24 SECTION 1 INTRODUCTION TO THE DATA PROTECTION ACT 1998 AND LEGAL BACKGROUND

1. BACKGROUND

2. WHAT IS THIS GUIDE FOR?

3. PERSONAL AND DEPARTMENTAL RESPONSIBILITY

4. PERSONAL INFORMATION

4.1. Departmental Policy

4.2. Information about staff

5. LEGAL BACKGROUND

5.1. Common law obligations of confidentiality

5.2. Human Rights Act 1998

5.3. Proportionality

6. DATA PROTECTION ACT 1998

6.1. The Data Protection Principles

6.2. The First Data Protection Principle (Fair And Lawful Processing)

6.3. Lawful

6.4. Fair

6.5. Conditions For Processing

6.7. Consent

6.8. The Second Data Protection Principle

6.9. Exemptions to the requirements of the DPA

7. FREEDOM OF INFORMATION ACT (FOIA) 2000

8. LEGAL POWERS TO DISCLOSE

8.1. **Court Orders**

8.2. **Common Law Powers**

8.3. **Statutory Powers**

8.4 **Statutory Gateways**

8.5 **Immigration and Asylum Act 1999 Data Gateways**

8.6. **Specified purposes in the Immigration and Asylum Act 1999**

8.7 **Nationality, Immigration and Asylum Act 2002**

8.8 **Immigration, Asylum and Nationality Act 2006**

8.9 **UK Borders Act 2007**

8.10 **Confidentiality and criminal penalty for wrongful disclosure of HMRC information**

9. **LEGAL PROHIBITIONS ON DISCLOSURE**

**CHAPTER 24
SECTION 1****INTRODUCTION AND LEGAL BACKGROUND****1. BACKGROUND**

This guide contains advice on when personal information may be disclosed by UK Border Agency staff. It is split into 13 Sections.

It has been produced by UK Border Agency's Information Access Policy Team in consultation with other stakeholders including Business Enquiry Service, Evidence and Enquiry (BES E&E); Data Protection Unit (DPU); Asylum Policy Unit (APU); Managed Migration Strategic Review (MMSR); National Asylum Support Service (NASS) and Legal Advisers Branch (LAB).

The guide is for use throughout the UK Border Agency (UKBA). Any questions about this guide should be directed to the UK Border Agency's Information Access Policy Team (IAPT) [<mailto:Freedom.Informationteam@homeoffice.gsi.gov.uk>].

2. WHAT IS THIS GUIDE FOR?

There have been many developments in the field of information disclosure in recent years, not least the coming into force of the Data Protection Act 1998 (DPA) and the implementation on 1 January 2005 of the main access provisions of the Freedom of Information Act 2000. The Immigration and Asylum Act 1999, the Nationality, Immigration and Asylum Act 2002, Immigration and Asylum Act 2006 and the UK Borders Act 2007 also contain a number of provisions regarding the disclosure and collection of personal information by the UK Border Agency relating to a range of specified circumstances and conditions. The increase in legislation in the area of disclosure has led to general increase in the number and variety of requests we receive for personal information from a range of sources, including other government departments, public authorities and third party individuals.

The guide contains an overview of the UK Border Agency's obligations and policy on the disclosure of personal information and guidance on when information relating to individuals (such as passengers and applicants) can be disclosed to third parties. It explains the balance between the obligation the UK Border Agency and its employees have to protect customer information and the need to disclose and share personal information when it is necessary to do so.

The management and disclosure of personal information is covered by a number of enactments, guidelines, policies, customs and practices which deal with the processing of (including disclosures of and access to) personal information relating directly to individual passengers, applicants, and members of staff. This can be broken down as follows:

- *Common law obligations of confidentiality*

- *The Human Rights Act 1998 (“HRA”)*
- *The Data Protection Act 1998 (“DPA”)*
- *The Immigration and Asylum Act 1999*
- *Nationality, Immigration and Asylum Act 2002*
- *Immigration, Asylum and Nationality Act 2006*
- *UK Borders Act 2007*
- *Internal security arrangements*
- *UKBA policy on the protection and disclosure of information; and*
- *The Freedom of Information Act 2000*

The Freedom of Information Act 2000 (“FOIA”) creates a statutory right to know about information held more generally by public authorities e.g. background on policy decisions or internal staff guidance. Further information on this and its relation to the disclosure of personal information is provided in this chapter. Section 12 of this chapter contains guidance on the interaction between the DPA and FOIA. Detailed guidance on FOIA can be found separately in IDI chapter 25.

Quick reference flowcharts setting out the stages to go through when considering requests for personal information or data are at Annex A1 and A2 to this section.

This guide takes account of the policy and legal background. If you follow the advice in this guide, or seek advice where the guide advises you to do so, the disclosures (and refusals to disclose) made will comply with both the UK Border Agency policy and the law. It is particularly important that UK Border Agency staff take care when handling personal information about individuals.

3. PERSONAL AND DEPARTMENTAL RESPONSIBILITY

If staff act properly within their authorised duties, and follow this and any other relevant instructions, responsibility would normally lie with the department and **not** the individual. If UK Border Agency policies and guidance are being followed the department will support the member of staff in any claim made against them. If the decision to disclose is not within the authority of the member of staff or the disclosure was made contrary to UK Border Agency policies or guidance, then both the department **and** the individual may be deemed responsible. Unlawful disclosure of personal data can be considered to be gross misconduct and could lead to disciplinary proceedings.

If after consulting this guide a member of staff is still unsure whether or not it is appropriate to disclose information in a particular instance, **always** seek further guidance before making a decision, either from your line manager, your Directorate FOI specialist (for FOIA requests) [<http://I01hm020/ind/foi/index.asp>] or the UK Border Agency’s Information Access Policy Team [<mailto:Freedom.Informationteam@homeoffice.gsi.gov.uk>].

4. PERSONAL INFORMATION

4.1. Departmental Policy

The UK Border Agency's policy is that personal information relating to passengers, applicants and members of staff should not be disclosed to private persons or private bodies unless there is a legal obligation to do so.

However, there will be instances where other government departments, agencies, local authorities and other bodies request access to personal information held by the UK Border Agency to enable them to carry out their functions. The UK Border Agency will consider all requests for personal information carefully and will comply where it is lawful to do so. Immigration application forms include a notification to applicants to that effect. Other government bodies have similar declarations on their application forms about disclosing information to the UK Border Agency for immigration and nationality purposes.

Under the DPA, individuals have a legal right of access to personal data we hold on them. ***[For further information on subject access rights and guidance on handling subject access requests see section 10].***

4.2. Information about staff

If a request for personal information about a member of staff is received, whether from the police, a body with statutory power of investigation or a relative, it should be referred to the Human Resources Directorate or the UK Border Agency Security Unit if appropriate for advice. **Do not** give any information or supply any documents without their authority. Chapter 25, section 12 contains further guidance about how to handle requests for information made under the FOIA by third parties concerning UK Border Agency staff or staffing numbers.

5. LEGAL BACKGROUND

Of particular relevance where disclosures of personal information are contemplated are common law obligations of confidentiality, the HRA, the DPA and FOIA. The administrative law requirement that public bodies must act within the limits of their powers is also relevant. These are considered in turn below.¹

5.1. Common law obligations of confidentiality

Personal information given to the department by individuals in connection with their applications for leave to enter and remain, asylum, citizenship and

¹ Staff should also be aware that, when considering the disclosure of information provided to the department by HM Revenue and Customs (HMRC), wrongful disclosure of that information is a criminal offence carrying a maximum penalty of up to 2 years imprisonment and an unlimited fine. See paragraphs 8.9 - 8.10 below and IDI section 3 for more details.

humanitarian protection that is not in the public domain may attract an obligation of confidentiality under common law.

In summary, information will be protected by the law of confidence if:

- it has the necessary quality of confidence – i.e. it is not in the public domain or readily available from another source, and has some sensitivity or value; and
- it was communicated in circumstances imparting an obligation of confidence.

Information subject to such an obligation may only be disclosed (a) if the individual consents, (b) if there is a legal obligation to make the disclosure in question, or (c) if there is an overriding public interest in the disclosure which outweighs the public interest in maintaining confidentiality.

It is open to aggrieved individuals to take legal action against the department claiming damages (compensation) for breach of confidence.

5.2. **Human Rights Act 1998**

The Human Rights Act 1998 (HRA) incorporates the European Convention on Human Rights (ECHR) into UK law. It requires public authorities to act compatibly with rights and freedoms set out in the ECHR, and enables people to enforce those rights in the UK courts in the first instance rather than the Court in Strasbourg. It also requires that all legislation must be interpreted, so far as is possible to do so, in a way, which is compatible with the Convention rights.

Article 8 of the ECHR states that everyone has the right to respect for private and family life, home and correspondence, and that there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the pursuit of a legitimate aim (these aims are specified in Article 8 and are set out below).

Article 8 is broad in scope and covers a wide range of activities including collection, use and disclosure of personal information relating to any individual.

The Article 8 right is not absolute. A public authority may interfere with this right where the interference is in accordance with the law **and** it is necessary:

- in the interests of:
 - national security;
 - public safety; or
 - the economic well-being of the country;
- for the prevention of disorder or crime;
- for the protection of health or morals; or
- for the protection of the rights or freedoms of others.

5.3. **Proportionality**

Case law from the Strasbourg Court indicates that in determining whether an interference is “necessary in a democratic society” in pursuit of one of the legitimate aims, “there must be a reasonable relationship between the aim to be achieved and the means used”, i.e. the interference must be proportionate to the aim pursued.

In the case of a request for personal information by another body, the disclosure of the information requested must be reasonable and proportionate to the purpose for which it is required. Caseworkers and Immigration Officers should bear in mind the need to disclose no more information than is necessary to achieve the object behind the request, and should ask themselves whether it is necessary to disclose all the information requested or whether it would be sufficient to disclose only some of it. For example, it may only be necessary to disclose a person’s address, date of their entry into the UK and/or whether they enjoy settled status here as opposed to full details of their application or status.

The majority of cases in which the UK Border Agency is asked to disclose personal information relate to the detection or prevention of crime, legal proceedings or the exercise of another public body’s functions. Where the police request access to UK Border Agency records for the purpose of investigating criminal offences, this may merit access to the whole of an applicant’s file, depending on the circumstances.

6. **DATA PROTECTION ACT 1998**

The Data Protection Act 1998 (DPA) regulates the “processing” of “personal data”. “Processing” means doing essentially anything with personal data, including collecting, holding, using, disclosing and destroying them. “Personal data” are “data” relating to identified or identifiable living individuals, where “data” means:

- a) any information held on any UKBA computer
- b) all recorded information held on manual files or
- c) any other recorded information held by UKBA

The definition of “personal data” also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Data do not have to relate solely to one individual and the same set of data may relate to two or more people and still be personal data about each of them. For example, joint tenants of a property or holders of a joint bank account or even individuals who use the same telephone or e-mail address.

The requirements set out in the DPA apply to “data controllers”. Each government department is a separate data controller, therefore the Home Office is the data controller of personal data held by IND. Where personal information is requested by another person or body, if that information constitutes “personal data” within the meaning of the DPA, the information can only be disclosed by the UK Border Agency if the disclosure would be

consistent with the requirements of the DPA, or if an exemption to those requirements applies.

Where personal information which constitutes “personal data” is requested by the individual to whom the information relates, the individual’s rights and the department’s obligations will be governed by the subject access provisions of the DPA, which are explained in more detail in section 10 of this chapter.

If a request is made regarding a deceased individual we do not need concern ourselves with the DPA (which applies only to personal data relating to living individuals), however a duty of confidentiality may remain under common law. Staff should seek guidance from the IAPT in dealing with any such request.

6.1. The Data Protection Principles

The DPA requires data controllers to comply with eight rules of good information handling known as the “data protection principles”. These are set out in Schedule 1 to the Act (with detailed interpretative provisions at Part II of Schedule 1), and provide as follows:

1. *Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-*
 - (a) *at least one of the conditions in Schedule 2 is met, and*
 - (b) *in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met. (The meaning of “sensitive personal data” is set out below.)*
2. *Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.*
3. *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*
4. *Personal data shall be accurate and, where necessary, kept up to date.*
5. *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*
6. *Personal data shall be processed in accordance with the rights of data subjects under this Act.*
7. *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*
8. *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. **[For more information on the eighth principle see section 9].***

The first and second principles are of particular relevance when making disclosures of information and are considered in more detail below.

Not all the Data Protection principles apply to data which is held other than on a computer or in relevant filing systems- this relates to section 33A of the Data Protection Act. Contact the IAPT for further information on this section of the Data Protection Act.

6.2. **The First Data Protection Principle (Fair And Lawful Processing)**

The first principle states that data must be processed fairly and lawfully **and** shall not be processed unless one of the conditions in Schedule 2 is met, and, in the case of sensitive personal data, one of the conditions in Schedule 3 is also met. This principle **must** be considered every time a request for disclosure of personal data is made.

There are exemptions to the requirements of the first data principle, however these do not provide exemption from the requirement to meet a Schedule 2 (and 3) condition, which must therefore always be complied with. [For more details about the exemptions in the DPA see below]. ***[More detailed information about disclosure to third parties including the police and other government departments can be found in section 3]***

6.3. **Lawful**

The requirement that processing must be "lawful" means that the processing in question (e.g. a particular disclosure) must be in accordance with all relevant rules of law whether derived from statute or common law (such as the law of confidence, considered at 5.1 above). Government departments derive their powers from many sources. Many public bodies, for example, government and statutory organisations, deal with personal data in order to carry out specific functions. In doing so they must act within the limits of their powers. Such powers may be set out expressly in statute, be implied from statutory provisions, or derive from the common law. Public bodies should be aware of the extent of their powers, in particular any specific restrictions on the use or disclosure of data. Where personal data are processed in a manner or for a purpose which is outside those powers then the processing will be unlawful. For further detail on powers for the UK Border Agency to make disclosures see part 8 below.

6.4. **Fair**

The first principle also requires that the processing must be "fair", which means that the individual must have, be provided with, or have made readily available to him, certain information, in particular information as to the purpose or purposes for which his/her data are being or may be processed. All immigration application forms include a declaration and although the wording may vary slightly, the meaning is the same. For example the Statement of Evidence Form for an asylum applicant indicates that:

“In deciding your claim, we keep the information you give us confidential. We will disclose nothing about your claim to the authorities of your own country. But we may disclose information to international organisations and other Government departments or agencies, local authorities, and other bodies in the UK to enable them to do their work. We may also disclose information in confidence to the asylum authorities of other countries that may be responsible for considering your claim”

6.5. **Conditions for Processing**

The other requirement of the first principle is that one of the conditions for processing in schedule 2 must be met, and one of the conditions in schedule 3 if sensitive personal data are involved.

Schedule 2

When dealing with basic personal data (e.g. name, address and date of birth), it will only be necessary to meet a condition under schedule 2. When disclosing such personal data one of the conditions under schedule 2 **must** apply.

The conditions, which are most likely to be relevant for IND purposes, are:

1. *The data subject has given his consent to the processing*

3. *The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.*

5. *The processing is necessary*
 - (a) *for the administration of justice,*

 - (b) *for the exercise of any functions conferred on any person by or under any enactment,*

 - (c) *for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or*

 - (d) *for the exercise of any other functions of a public nature exercised in the public interest by any person.*

6. (1) *The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.*

The conditions which are most likely to cover disclosure of personal data in response to requests by other government bodies or local authorities are those set out in 5(b), (c) and (d), and 6(1).

It should be noted that “necessary” in the context of the schedule 2 and 3 conditions could be interpreted broadly, to mean “reasonably required in connection with” rather than “absolutely essential for”.

Schedule 3

Schedule 3 sets out the conditions for processing sensitive personal data, which are defined as personal data consisting of information as to:

- (a) the racial or ethnic origin of the data subject;
- (b) his political opinions;
- (c) his religious beliefs or other beliefs of a similar nature;
- (d) whether he is a member of a trade union;
- (e) his physical or mental health or condition;
- (f) his sexual life;
- (g) the commission or alleged commission by him of any offence; or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

When disclosing sensitive personal data one of the conditions under schedule 3 **must** be met (in addition to a condition under schedule 2).

The conditions, which are likely to be most relevant for UK Border Agency purposes, are:

1. The subject has given his explicit consent

6. The processing-

(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.

7. - (1) The processing is necessary-

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

6.6. Elected representatives

Further circumstances in which sensitive personal data may be processed may be provided for in secondary legislation made by the Lord Chancellor. Two orders have been made under this power, one containing a variety of

conditions in which sensitive personal data may be “processed” (S.I. 2000 No. 417), and one relating specifically to disclosures made by and to elected representatives (S.I. 2002 No. 2905).

In particular, S.I. 2000 No 417 covers (in paragraphs 1 and 10 of the Schedule) cases where:

1. *The processing-*
 - (a) *is in the substantial public interest,*
 - (b) *is necessary for the purposes of the prevention or detection of any unlawful act, and*
 - (c) *must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.*
10. *The processing is necessary for the exercise of any functions conferred on a constable by any rule of law.*

[Further information concerning the disclosure of personal information to MPs can be found in section 4 of this IDI].

6.7. **Consent**

One of the conditions for processing data that features in both schedule 2 and 3 is that the processing be carried out with the consent of the individual concerned (although in the context of the schedule 3 condition the consent must be “explicit”). For the purposes of schedule 2 consent can either be obtained each time disclosure is deemed necessary or can be implied by the individual signing a declaration on original application form permitting further disclosure of their data to named organisations for specific purposes. However, schedule 3 states “*The data subject has given his **explicit** consent to the processing of the personal data*” therefore if consent is to be relied upon before disclosure the individual **must** be asked for his explicit consent before disclosure can take place in every instance. Caseworkers and IOs should also consider whether to seek the subject’s consent when none of the other conditions in schedule 2 or 3 are satisfied.

6.8. **The Second Data Protection Principle**

This principle states that personal data must be obtained only for specified and lawful purposes, and must not be further processed in any manner incompatible with those purposes. The requirement of compatibility in this context has a relatively low threshold. Compatible does not mean “identical to”, and purposes which are quite different from the original purposes can still be compatible with those original purposes. Therefore, provided the further processing is for a purpose that is not contradictory to the originally specified purpose or purposes, it will be consistent with the second principle.

6.9. Exemptions to the requirements of the DPA

The DPA makes provision for a number of exemptions to its requirements, however it must be noted that each exemption is very specific as to the provisions to which it applies and the circumstances in which it applies.

The exemptions which may be relevant for the UK Border Agency's purposes are-

- (a) The **national security** exemption (section 28) – provides exemption from essentially any of the provisions of the DPA, insofar as exemption from the provision is required for the purpose of safeguarding national security
- (b) The **crime** and **taxation** exemption (section 29) - provides that personal data processed for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty, are exempt from the first principle in any case to which the application of this provision would be likely to prejudice any of these matters. (This does not exempt the data controller from the obligation to comply with conditions in Schedules 2 and 3). In order to rely on this exemption, you must therefore be satisfied that the disclosure of the requested data is for one of these purposes and that applying the fair processing requirement would be likely to prejudice that purpose.
- (c) The **required by law** and **legal proceedings** exemption (section 35) – this exempts personal data from the non-disclosure provisions where the disclosure is required by a statutory provision, or an order of a court, or where disclosure is required for the purpose of, or in connection with, legal proceedings or for the purpose of obtaining legal advice, or for otherwise establishing, exercising or defending legal rights.

7. FREEDOM OF INFORMATION ACT (FOIA) 2000

The main statutory access provisions of the FOIA were brought into force on 1 January 2005. These create a statutory basis which allows any member of the public **the right to know** whether a public authority holds information requested, and allows them to have access to that information providing it is available and not subject to any exemptions. FOIA only applies to information which does not fall under either the DPA or the Environmental Information Regulations 2004. While the DPA sets out how we deal with information about living individuals and their personal data, the FOIA is generally concerned with all other information, although it also creates access rights to information for third parties which may involve the disclosure of personal data.

The provisions of the FOIA complement the DPA and the other rules which govern the way we retain and disclose personal information. Section 40 of the FOIA is the most salient provision in respect of disclosing personal data to third parties, as it sets out a potential exemption from the **right to know**

where the information requested by a third party may consist of personal data:

- Under Section 40 (1) of the FOIA, if the personal data requested is about the person requesting the information, then there is no right to know under the FOIA - such requests are routed by section 40(1) to the subject access regime of the DPA. In such cases the exemption to the FOIA is absolute- there is no need to consider the public interest balancing process **[see sections 11 & 12 for further details of how to handle such requests]**
- Section 40 (3) of the FOIA, deals with requests for information about a living individual from someone other than that person. Section 40(2&3) exempts that information from disclosure if disclosure would breach, amongst other things, the Data Protection principles (see part 6.1 of this section for a full explanation of how section 40(3) works)

For further detailed information on dealing with requests for personal information made under the FOIA, please refer to section 12 of this IDI and chapter 25, section 12 for more detail.

8 LEGAL POWERS TO DISCLOSE

The lawful basis (i.e. power) for the UK Border Agency to make a disclosure can be derived from a number of sources.

8.1. Court Orders

Disclosure ordered by UK Courts will invariably be lawful. Court orders must be complied with unless the issue of Public Interest Immunity arises. **[Further information about PII can be found in section 6].**

8.2. Common Law Powers

As a general rule, government departments headed by a Crown Minister including the Home Office, DWP, Department for Transport, etc may disclose any data unless the disclosure is prohibited by statute. This derives from the principle that the Crown has the power to do anything that an ordinary person has power to do unless prohibited by statute, whether expressly or implied. This means that unless there is an express or implied statutory prohibition on a particular disclosure, the UK Border Agency (or any other ministerial department) will have the power to make the disclosure. This relates to the information flow both to the UK Border Agency from other ministerial departments, and by the UK Border Agency to any other bodies including government departments (whether ministerial or non-ministerial), local authorities and where appropriate foreign governments. These are referred to as our **"Ram Powers"**.

8.3. **Statutory Powers**

Some departments (such as HM Revenue & Customs) are created by statute and are not headed by a Crown Minister. They derive all their powers from statute, those powers may be set out expressly or implied as reasonably incidental to express statutory functions. It is a matter of statutory construction in each case as to whether a particular statute permits disclosure for the particular purpose or purposes contemplated.

8.4 **Statutory Gateways**

In some areas to provide clarity or to provide a lawful basis for processing which would not otherwise exist, Acts of Parliament make express provision for data disclosures or exchanges via statutory gateways. The Immigration and Asylum Act 1999 provides reciprocal gateways between the UK Border Agency, Chief Officers of police, the Serious Organised Crime Agency (SOCA) and HM Revenue & Customs for specified purposes. The UK Borders Act 2007 also created new powers and obligations in this field in relation to HM Revenue & Customs.

8.5 **Immigration and Asylum Act 1999 Data Gateways**

Sections 20 and 21 of the Immigration and Asylum Act 1999 provide a lawful basis for reciprocal information exchanges between the UK Border Agency, the police and SOCA for specified purposes. Section 21 also provides a lawful basis for the disclosure of UK Border Agency information to HM Revenue & Customs for “customs purposes” as defined in s21. The existence of the legal power does not obviate the need to comply with the HRA and the DPA.

8.6. **Specified purposes in the Immigration and Asylum Act 1999**

“Immigration purposes” for which UKBA may be supplied information are defined as:

- (a) the administration of immigration control under the Immigration Acts;
- (b) the prevention, detection, investigation or prosecution of criminal offences under those Acts; (This includes **all** immigration offences such as absconding, working in breach, illegal entry etc)
- (c) the imposition of penalties or charges under Part II of the Immigration and Asylum Act 1999 (Carriers Liability)
- (d) the provision of support for asylum-seekers and their dependants under Part VI of the Act (support for asylum-seekers)
- (e) such other purpose as may be specified in an order made by the Secretary of State (no such orders have yet been made).

“Police purposes” for which the police may be supplied information are defined as:

- (a) The prevention, detection, investigation or prosecution of criminal offences
- (b) Safeguarding national security;

- (c) Such other purposes as may be specified (Other police purposes can be defined by the Secretary of State, but to date none have).

“SOCA purposes” for which SOCA may be supplied information are defined as:

any of the functions of the Serious Organised Crime Agency mentioned in section 2, 3 or 5 of the Serious Organised Crime and Police Act 2005.

“Customs purposes” for which HMRC may be supplied information are defined as:

- (a) the prevention, detection, investigation or prosecution of criminal offences;
- (b) the prevention, detection, investigation of conduct of which penalties which are not criminal penalties are provided for by or under any enactment;
- (c) the assessment or determination of penalties which are not criminal penalties;
- (d) checking the accuracy of information relating to, or provided for purposes connected with, any matter under the care of the Commissioners or any assigned matter (as defined by section (1) of the Customs and Excise management Act 1979) ;
- (e) amending or supplementing any such information (where appropriate);
- (f) legal or other proceedings relating to anything mentioned in paragraphs (a) to (e)
- (g) safeguarding national security; and
- (h) Such other purposes as may be specified (no such purposes have yet been specified).

8.7 Nationality, Immigration and Asylum Act 2002

Sections 134-139 of the Nationality, Immigration and Asylum Act 2002 provide the UK Border Agency with the power to require employers and financial institutions to provide information about specified individuals suspected of committing certain immigration offences. The new powers include criminal penalties for non-compliance, and came into force on 30 July 2003. ***[More information about the extent and usage of these powers can be found at section 3].***

8.8 Immigration, Asylum and Nationality Act 2006

Section 36 of this Act created a new coercive power to share information between the border agencies i.e. the UK Border Agency, HMRC and the police. For further information on this coercive information sharing gateway staff should contact Border Control Policy Implementation (BCPI).

8.9 UK Borders Act 2007

The UK Borders Act (s40) created a new consolidated, wider gateway for HMRC to provide information to the UK Border Agency for specified purposes. The new powers came into effect on 31 January 2008. HMRC officers may now share information with the UK Border Agency if it is required for any of the following purposes:

- administering immigration control under the Immigration Acts;
- preventing, detecting, investigating or prosecuting offences under those Acts;
- determining whether to impose penalties on carriers (under Part II of the Immigration & Asylum Act 1999);
- determining whether to impose penalties on employers who employ illegal migrant workers (section 15 Immigration, Asylum and Nationality Act 2006);
- providing accommodation or support to families or asylum seekers and their dependents
- determining whether a person applying for British citizenship is of “good character” (under the British Nationality Act 1981 or the Immigration, Asylum and Nationality Act 2006);
- determining whether to deprive a person of their British citizenship (section 40 of the British Nationality Act); or
- anything else in connection with the exercise of “immigration and nationality functions” (as defined in the UK Borders Act).

This means that HMRC officers have the requisite power, for example, to provide information to UKBA to enable staff to make robust case work decisions e.g. checking whether an applicant has breached previous leave by working illegally or unlawfully claiming benefits, verifying information provided by sponsors or for preventing/detecting asylum support fraud. Staff must still ensure that any request for information from HMRC is necessary and proportionate (see paragraphs 5 & 6 above) and that requests are made in line with the published MoU [*see section 3 of this IDI*].

8.10 **Confidentiality and criminal penalty for wrongful disclosure of HMRC information**

Section 41 of the UK Borders Act is a statutory duty of confidentiality for all HMRC information provided to the UK Border Agency. This means that HMRC information cannot be disclosed by UK Border Agency staff to anyone outside the department except in certain circumstances (see below). This includes information provided by HMRC prior to the commencement of these new powers (i.e. prior to 31 January 2008).

Section 42 of the UK Borders Act creates a criminal offence for disclosure of HMRC information in breach of the statutory duty of confidentiality. Staff may be individually prosecuted for breach of this duty. Conviction for a wrongful disclosure of HMRC information carries a penalty of up to 2 years imprisonment and an unlimited fine. Ignorance of this offence cannot be used as a defence against prosecution.

For this reason staff must ensure that HMRC information is clearly marked as such so that it is not accidentally shared outside the UK Border Agency. It is

strongly suggested that all HMRC information is clearly marked with the following: “RESTRICTED - HMRC (see MoU)”. Staff must also ensure that when considering a disclosure of HMRC information to another body/person outside the UK Border Agency, the disclosure is permitted by law.

From 31 January 2008 staff may only disclose information provided by HMRC to a person or organisation outside the UK Border Agency in the following circumstances:

- where necessary for any of the purposes listed at paragraph 8.9 (i.e. those set out in section 40 of the UK Borders Act);
- where necessary for the purpose of civil proceedings relating to an immigration or nationality matter e.g. an immigration appeal;
- where necessary for the purpose of criminal proceedings relating to an immigration or nationality matter e.g. prosecution for immigration offences;
- where we are required to do so by a court order;
- where we have the written consent of HMRC to do so;
- where we have the written consent of the person to whom the information relates to do so; or
- where the disclosure is permitted in another enactment e.g. to the police or SOCA under section 21 of the Immigration and Asylum Act 1999 or to the “border agencies” under section 36 of the Immigration, Asylum and Nationality Act 2006. ***NB: staff must seek the approval of the HMRC Gateway Exchange Team (London – paul.k.wright@hmrc.gsi.gov.uk) prior to making such disclosures.***

If in doubt about disclosing information provided by HMRC staff must always seek advice from the IAPT (0208 760 4657).

9 LEGAL PROHIBITIONS ON DISCLOSURE

Staff should be aware that in some circumstances information is protected from disclosure by specific legislation. The Gender Recognition Act 2004 (GRA) makes it illegal for a civil servant to disclose the previous identity of a person who has acquired a new gender and has a gender recognition certificate. Disclosure of the previous identity of such an individual, except in certain specified circumstances, could result in the individual or organisation being given a fine of up to £5000 and a criminal record. ***[More information on the GRA can be found in IDI chapter 16].***

