Code of Practice on the management of information shared by the Border and Immigration Agency, Her Majesty's Revenue and Customs and the Police

Presented to Parliament by the Secretary of State for the Home Department and the Treasury under section 37 of the Immigration, Asylum and Nationality Act 2006

CONTENTS

Section 1

Foreword

The White Paper "One Step Ahead – A 21st Century Strategy to Defeat Organised Crime" tasked the three main UK border agencies - the Border and Immigration Agency, Her Majesty's Revenue and Customs (HMRC) and the Police - to work more effectively together to create a secure integrated border.

It also highlighted the importance of achieving the ambition of improving the agencies' ability to capture and share traffic data about goods and people crossing our border. Paragraph 3.2.1 of the White Paper states: "improving this (data capture and sharing) is fundamental to the ability of all of the frontier agencies to identify and separate from the mass of legitimate traffic crossing our borders that which poses a risk." It concludes: "there is a need to identify and overcome other obstacles to maximising the potential for joint data capture and sharing, including legal constraints…"

A key element of delivering this closer working as identified by the White Paper is ensuring that information about people and freight crossing the border is captured efficiently by the border agencies and shared between them effectively. This will increase the border agencies' ability to identify and target those individuals who present a threat to the UK and to mount an appropriate, co-ordinated and proportionate response whilst facilitating the free flow of legitimate travellers through the UK border controls.

In response to the White Paper findings, the Immigration, Asylum and Nationality Act (the IAN Act) 2006 created new passenger, crew, service and freight data acquisition powers for the police, and extended and enhanced the powers of the Border and Immigration Agency and HMRC to require this type of data in advance of arrival. It also introduced a duty requiring the effective sharing of this information between the border agencies.

These powers will enhance the border agencies' ability to establish, in advance of travel, the level of threat posed by an individual or freight movement and tailor the appropriate operational response. This is a key component of an intelligence-led risk-based approach to border control.

This Code of Practice details how the legislative framework will be implemented, how personal information will be used and the safeguards for the use of this data. It provides the basis for reliable, secure and effective information management by the border agencies. It shall be supplemented through a consistent and wide range of further guidance, methods, checklists and tools. This is a dynamic and evolving code that will be subject to periodic review, (the first of which will be six months after publication), and will be updated as necessary.

The Prime Minister announced on 14 November a wide range of measures to counter terrorism and strengthen border security, including the establishment of a UK Border Agency. The new Agency will bring together the work of the Border and Immigration Agency, UKvisas and the detection work at the border of HM Revenue & Customs into a single organisation responsible for tackling smuggling as well as immigration control. It will report jointly to the Home Secretary and the Chancellor of the Exchequer on its work at the border – managing the flow of goods and people. The Prime Minister's announcement also foreshadowed further work on the role of policing at the border, to be led by the Home Secretary working jointly with the Association of Chief Police Officers (ACPO) and the Association of Chief Police Officers in Scotland (ACPOS).

This integrated approach signals a step change in the Government's commitment to strengthening border security through joint working and reinforces the essential role that efficient and effective sharing of passenger, crew and freight-related information plays in its delivery. The Government will legislate to create the new agency as soon as Parliamentary time allows. In the meantime, the provisions in the IAN Act 2006, as governed by this Code of Practice, will provide the legislative framework for data capture and sharing to support closer working at the border.

Section 2

2.1 Introduction

The Immigration Asylum and Nationality (IAN) Act 2006 introduced provisions at section 36 to underpin the data sharing required by the UK border agencies under e-Borders[1] and other joint working arrangements. These require the Secretary of State for the Home Department (in so far as she has functions under the Immigration Acts), Her Majesty's Revenue and Customs and a chief officer of police ("the border agencies") to share certain passenger, crew, service, freight and other travel related information between them, where that information is likely to be of use for immigration, police or HMRC purposes.

Section 37 of the same Act created a requirement for the Secretary of State and Treasury to jointly issue one or more codes of practice about:

- the use of information shared in accordance with section 36(2); and
- the extent to which, or form and manner in which, shared information is to be made available in accordance with section 36(6)[2].

Each of the border agencies has given consideration to the data which is likely to be of use for immigration, police or HMRC purposes, based on the operational needs of the individual agencies. They are satisfied that information to be shared under section 36 of the IAN Act 2006 meets that test. The border agencies regard the lawful and proportionate processing of personal information as necessary for the successful delivery of their aims and to maintain confidence in the border agencies by the public.

Border security is dynamic, evolving and reactive. Consequently - and in order to ensure maximum protection of individuals' data - the data elements to be shared between the agencies will be kept under review. This will ensure that the section 36 test will continue to be satisfied and that information will be removed from the section 36 requirement where appropriate. In addition, this Code of Practice will be reviewed periodically, and the use of data will be closely monitored and auditable.

2.2 Aim and scope of code

This Code of Practice meets the requirement of section 37 of the IAN Act 2006 by making provision about how information will be shared between the border agencies under section 36 of the same Act and about safeguards to be implemented with regard to such sharing. It also aims to provide reassurance and confidence in respect of how personal data will be used and stored; it also details specific working arrangements that will be put in place to assist individuals in making subject access requests (SARs).

[1] See page 14.
[2] See annex A for details of section 36-37 of the IAN Act 2006.

This Code covers a range of joint working arrangements, including e-Borders, and will establish the key principles to be reflected in arrangement-specific operational guidance for border agency officers.

The scope of this Code of Practice is limited by the parameters of the duty to share legislation as defined in section 36 of the IAN Act 2006. **It does not cover any sharing of information by or between the border agencies outside the terms of section 36 of the IAN Act 2006 or the onward sharing of information obtained under section 36 via other powers. Section 36 does not seek to restrict existing powers of the border agencies to share data.**

2.3 Who is covered by the Code?

This code covers data sharing between the Border and Immigration Agency, Her Majesty's Revenue and Customs, the Police and UKvisas[3].

2.4 Duty to share

The duty to share under section 36 of the IAN Act 2006 applies to information which is acquired under powers, or which relates to matters, which are specified by order of the Secretary of State and Treasury under that section.

The border agencies must share such information only to the extent that it is likely to be of use for immigration, police or Revenue and Customs purposes as defined in the Immigration and Asylum Act 1999. These purposes are set out at Annex B. The information shared under section 36 of the IAN Act 2006 will be used by the border agencies for clear, specified objectives which are necessary and relevant to the aims of the border agencies.

2.4.1 Application to Scotland

The statutory duty to share data applies to the border agencies throughout the United Kingdom. However, the purposes for which a chief officer of police in Scotland is required to share the information are more limited than in other cases.

Section 36(3) of the IAN Act 2006 allows a chief officer of police in Scotland to share information only to the extent that it is likely to be of use for:

- immigration purposes;
- police purposes, in so far as they are or relate to reserved matters within the meaning of the Scotland Act 1998 (c.46); or
- Revenue and Customs purposes other than the prosecution of crime.

[3] UKvisas is currently a joint Foreign and Commonwealth Office/Home Office operation. On 25 July 2007 the Prime Minister announced the decision to merge UKvisas with the Border and Immigration Agency. The merger will be phased over the next few months to be completed by April 2008. At present, the Secretary of State obtains and holds information pursuant to her functions under the Immigration Acts through both the Border and Immigration Agency and UKvisas.

Section 3

3.1 Why information will be shared between the border agencies

Although the border agencies each have different core functions in respect of border control, these comprise a number of key and frequently interdependent (although complementary) components across all border agencies, including a counter terrorism strategy, initiatives to combat organised crime and strategies to enforce Immigration and Customs controls.

A principal aim of joint working arrangements is to enhance the capabilities of the border agencies to deliver a secure integrated border. One agency for example may have intelligence or information about an individual or a company which is not known to the others, but which may prove to be of interest to them. Awareness of this information could be the crucial factor which influences a decision as to whether or not to mount an intervention.

Operational experience has proven that there is a significant degree of commonality between the passenger and freight data elements used by the border agencies to identify movements of interest to them. This reinforces the need to ensure that adequate capabilities exist for them to share and analyse that data in a co-ordinated manner.

The information to be shared [section 3.3] will be used by the border agencies for clear, specified objectives [section 3.5]. The information to be shared is necessary for, and relevant to the aims of the border agencies; the information to be shared is necessary for alerting the border agencies to both a) individuals already identified as being of interest and b) patterns of activity that appear unusual and require further investigation. The information to be shared between the agencies is proportionate. In accordance with section 36 of the IAN Act 2006, it does not go beyond that which is likely to be of use for immigration, police or Revenue and Customs purposes.

The border agencies have worked in operational and intelligence partnerships for many years. Legislation requires each agency to collect information only where it is necessary for its functions. Experience has shown that data captured from carriers under immigration, police and customs legislation and other information held in agency systems can, when brought together develop intelligence and support more effective action. Indeed Project Semaphore[4], the e-Borders pilot, has proved that the data that will be subject to the duty to share has been of immense value to the border agencies in carrying out their functions.

[4] Project Semaphore is the pilot project for e-Borders which currently screens 29 million passenger movements (annualised). Over 16,500 alerts have been issued, with 1300 arrests.

Whilst not every piece of data shared between the agencies will be used in every case, any of the pieces of data shared is likely to be of use for one or more agency purposes; it is not possible to predict in advance of obtaining the data which elements will be required in which cases. It is for that reason that the information must be obtained in bulk and its use will then vary on a case by case basis. The border agencies are able to identify the information that will be of use, based on both current operational knowledge and experience and the circumstances at the time.

This section sets out:

3.2 The legal provisions for sharing
3.3 The information that will be shared
3.4 The form and manner of information to be shared between the border agencies
3.5 The purpose of information sharing
3.6 How information will be shared in practice.

3.2 Legal provisions for sharing

The information to be shared in accordance with section 36(2) of the IAN Act 2006 must be information which is:

(a) obtained or held in the exercise of a power specified by the Secretary of State and the Treasury jointly by order and which relates to passengers, crew or freight on a ship or aircraft or to a flight or voyage; or
(b) relates to other matters in respect of travel or freight as may be specified by the Secretary of State and the Treasury jointly by order.

The Secretary of State and the Treasury Minister may only make an order under section 36 of the IAN Act 2006 if satisfied that the sharing is likely to be of use for immigration, police or HMRC purposes and if there are likely to be circumstances in which it can be shared without breaching Convention rights (within the meaning of the Human Rights Act 1998 (c.42)).

The relevant order, the Immigration, Asylum and Nationality Act 2006 (Duty to Share Information and Disclosure of Information for Security Purposes) Order 2008, is to be laid before Parliament and subject to approval by both Houses of Parliament, will come into force on 1 March 2008.

The same information will also be shared in respect of trains arriving or departing the United Kingdom via the channel tunnel. This will be achieved by modifying and applying section 36 of the IAN Act 2006 and the order under that section to those trains in an order under section 11 of the Channel Tunnel Act 1987. The data acquisition powers specified in the section 36 order will also be modified and applied to trains in an order under section 11 of the 1987 Act. In this way, it will be possible to acquire passenger, crew, freight and service data in relation to trains arriving in and departing from the UK via the

Channel Tunnel and it will be possible to share that information pursuant to section 36 of the IAN Act 2006, as modified. References in this code to information relating to trains or to passengers, crew or freight on trains relates only to trains arriving and departing the United Kingdom via the channel tunnel.[5]

The terms of sections 36 and 37 of the IAN Act 2006 are set out in Annex A and matters specified in the 2008 order made under section 36 are set out in Annex C.

3.3 The information that will be shared

Generally speaking the information subject to the duty to share falls into three categories, set out below.

3.3.1 Category 1: Information about a passenger's or crew member's travel document or journey

This information can be broadly grouped into the following types:

a) Travel Document Information (TDI)[6]

Carriers will be required to collect and transmit all TDI data to the border agencies. TDI refers to a passenger's or crew member's biographic and travel document details, normally contained in the machine-readable zone of a passport or other travel document (details of which are set out below).

- Full name
- Gender
- Date of birth
- Nationality
- Type of travel document
- Travel document number
- Travel document issuing state
- Travel document expiry date

Where the passenger or a member of crew does not hold a travel document, information must be provided regarding the type of identification relied upon together with the number, expiry date and issuing State of that identification.[7]

[5] The IAN Act 2006 powers relate to ships and aircraft. In order to extend the data capture and sharing powers to trains, it is necessary to apply the relevant provisions with modifications to trains under powers in section 11 of the Channel Tunnel Act 1987. This position was made clear in the Regulatory Impact Assessment on data capture and sharing powers for the border agencies published on 28 February 2006.
[6] In the aviation industry this data is also known as Advance Passenger Information (API).
[7] Some categories of persons are able to travel without a travel document, for example those travelling on Military ID cards.

b) Other Passenger Information (OPI)[8]

OPI refers to information held by a carrier in connection with a passenger's booking or reservation. In the airline industry, this also includes data held within an airline's Departure Control System (DCS) such as check-in time, seat number and baggage details.[9]

The extent to which OPI is gathered by carriers varies both between and within different transport sectors. However, it is important to note that OPI data need only be supplied by the carrier to the extent that it is known to them. Carriers will not be required to supply OPI data elements that they do not ordinarily collect for their own commercial purposes.

OPI data is available in advance of a journey and therefore allows improved analysis and consequently better targeting of those of interest. This data will be used to identify suspects, their associates and behaviour in the travel process. This will be achieved by using the data as single items or by combining a number of elements to identify a pattern of behaviour or characteristics that make them worthy of further investigation.

OPI data is relevant and necessary to the aims of the border agencies; its use in detecting those of interest to the border agencies has been validated through Project Semaphore, and years of experience in utilising this data to target border criminality and profiles developed using that data.

A list of the OPI data to be requested is set out at annex D.

c) Service Information (SI)

Service information is information related to the flight, train or ship the passenger or crew member is travelling on. This information must be provided by the carriers in all cases for both inbound and outbound journeys:

- Flight number, train service number or ship name or carrier running number
- Name of carrier
- Nationality of ship
- Scheduled departure date and time
- Scheduled arrival date and time
- Place and country from which the flight, journey or voyage departed immediately prior to arrival into the United Kingdom
- Place in the United Kingdom where the flight, journey or voyage first arrives from overseas
- Any place in the United Kingdom where a flight, journey or voyage which has arrived into the United Kingdom from overseas will subsequently go
- Number of passengers.

[8] In the aviation industry this is also known as Passenger Name Record (PNR).
[9] In practice, OPI data will be routinely requested from carrier reservation and departure control systems in respect of the aviation industry; and from comparable maritime/rail systems.

d) Additional information regarding passenger's and crew vehicles and members of crew

Carriers will be required to submit the vehicle registration mark (VRM) in respect of any vehicle in which a passenger or member of crew is travelling and which is carried on a service or voyage, together with the registration number of any trailer attached to that vehicle**.**

Carriers will also be required to inform the Border and Immigration Agency of the number of crew on a flights, journey or voyage, the place of birth and rank of a member of crew.

3.3.2 Category 2: Information held by the border agencies, which relate to a passenger or crew member or their journey or a freight movement

This may include information such as historical data from previous journeys/movements or intelligence on suspect individuals/vehicles.

3.3.3 Category 3: Information about or related to freight

This will include details about the freight movement, including the parties involved in the transaction and details about the goods being moved (e.g. description, weight, origin, value, route taken to the UK etc).

3.4 Form and manner of information to be shared between the border agencies.

The form and manner in which the information will be made available to the border agencies and the procedures to manage that data will depend on the operational processes, technical infrastructure and border agency representation at each location. Consequently, information may be made available in a range of ways, including shared access to electronic databases and other electronic and manual processes. Although there are many ways in which the information may be shared there are robust safeguards for the protection of the data in every case.

3.5 Purposes of information sharing

Information shared in accordance with section 36(2) of the IAN Act 2006 will be used for the following purposes:

3.5.1 To identify those who present a threat to border security

Border control can have a direct impact on security and quality of life throughout the UK. Border control planning is directly linked to threats to the UK and by tightening our controls at the borders we have an opportunity to improve security across the UK as a whole. Shared data will be used to:

- identify individuals who are of a national security, smuggling, or immigration interest;
- identify individuals who are involved or suspected of being involved in crime;
- enforce judicial orders including warrant and those imposing travel restrictions;
- provide evidence of travel history and movements for judicial proceedings; and
- protect the vulnerable.

3.5.2 To determine a proportionate operational response

The ability to share data between the border agencies increases their ability to mount an appropriate, co-ordinated and proportionate response to any assessed threat.

Once analysed, travel data will benefit the border agencies in the following ways:

- To inform interventions by agencies
- To apprehend offenders
- To inform agency resourcing, strategy and policy development.

3.5.3 To detect crime

The Government recognises the value of Travel Document Information (TDI), Other Passenger Information (OPI) and other travel related data not only for border management but also for wider law enforcement activity. Data processing under these provisions has a valuable role to play in wider areas of law enforcement. For instance it can be used to track the movements and intended movements of known or suspected criminals.

3.5.4 Profiling and trend analysis

Acquiring passenger, crew and freight information in advance of travel or building a record of historical data on previous movements allows the border agencies to:

(a) analyse trends in passenger/freight movement; and
(b) build an intelligence picture of the behaviours of those involved in illicit activity.

This information can then be used by the border agencies to carry out risk assessments in support of their functions and determine appropriate levels of

intervention before any suspects arrive in the UK. This targeted approach has the potential to reduce delays at ports and ensure better use of resources: a more co-ordinated response by the border agencies will prevent the same passenger or vehicle being examined by each of the three agencies in turn. It will also allow persons of interest to be identified to the appropriate agencies in advance of their arrival in the UK, for example when they apply for a visa, and for appropriate, co-ordinated action to be taken.

The use of data in detecting those of interest to border agencies has been validated through Project Semaphore, and problem profiles have been developed using that data.

3.6 How information will be shared in practice.

The border agencies will use the data sharing powers from 1 March 2008 to support a range of joint working activities and Project Semaphore.

The practical arrangements in place for information sharing will vary according to a number of factors, including the nature of the joint working activity in which the agencies are engaged. Such joint activity may range from the fully integrated working envisaged for the purpose of processing and analysing bulk information within the e-Borders Operations Centre (e-BOC) to circumstances where the agencies are working together at a more local level and have a common interest in information about individuals and/or freight crossing the border concerned. The security of this information will always be first priority in all working arrangements.

3.6.1 e-Borders

e-Borders is the border agencies' strategic IT solution to the need for acquisition, joint pooling and analysis of electronic passenger, crew, service and freight information.

e-Borders will roll out from late 2008[10] and will introduce capabilities that support the delivery of a fundamentally more comprehensive, effective and efficient border control. It will support closer working between the agencies, with a particular emphasis on enhancing joint analytical capability. This will maximise the potential to identify individuals who present a threat to the United Kingdom and for the border agencies to mount an appropriate, co-ordinated and proportionate response.

The types of information collected from carriers (see 3.3.1) will be pooled into a single electronic database within the e-borders operations centre (e-BOC). The e-BOC will be jointly operated by the border control agencies. Data provided by carriers will be analyised, acted upon and disseminated as necessary.

Information will be made available to officers of the border agencies in the following ways:

[10] e-Borders will roll-out incrementally across air, sea and rail starting in late 2008. Full roll-out is expected by 2014.

- Data (see 3.3.1) will be made available electronically to officers of each border agency within the operations centre; and
- Border agency staff with appropriate security clearance within the operations centre will routinely be able to view the data, and make enrichments and interpretation of the data to produce alerts for dissemination.

Each of the border agencies will base staff in the operations centre who will jointly process and analyse the information by checking it against agency watch lists and against problem profiles to which the border agencies have shared access. Where matches are identified and confirmed as valid hits these hits will be further enriched with a wide range of information from agencies and alerts issued to the relevant agency where necessary. Data that has been enriched will be clearly identified allowing appropriate action and safeguards to be taken in respect of any further dissemination. This process will prevent interventions against those not of interest to the border agencies.

Data will be shared for the purposes of risk assessing departing and arriving passengers and crew at UK ports in order to enhance immigration, customs and border control procedures. Information will also be used for historical movement record checking, profiling and data mining for intelligence purposes. e-Borders will also provide watch listing functions to support improved background checking of applicants at overseas UK visa posts. System enquiries may also be made from other secure locations, including visa posts abroad.

Staff will act in accordance with the roles, responsibilities and powers they have and in accordance with operational instructions. Full management oversight will be in place, with regular audits by line managers.

3.6.2 Joint working arrangements outside e-Borders

Section 36 IAN Act 2006 and this Code of Practice also supports the border agencies working together under other arrangements where data-sharing is of paramount importance. These arrangements include small specialised teams of co-located officers that focus on collecting and generating intelligence about specific types of illicit activity, such as money laundering, the smuggling and distribution of firearms and offensive weapons and wildlife crime. Other working arrangements include units that undertake joint targeting specialising in identifying suspicious freight movements and issuing alerts to appropriate operational staff, and teams that specialise in building up intelligence on a variety of criminality in a specific geographical area. Staff working in these arrangements may be specifically recruited and operate in specific roles with appropriate access to information based on their roles. They will be subject to local supervision and auditing.

Section 4

4.1 Safeguards

The personal nature of the information to be shared under section 36 of the IAN Act 2006 requires that the information must be processed in a manner which is compliant with our obligations under the European Convention of Human Rights and in accordance with the Data Protection Act 1998.

This section will identify the key principles to which border agency officers will adhere in sharing and using that information. It will also demonstrate compliance with the relevant legislation: the European Convention on Human Rights (ECHR); the Data Protection Act 1998; and the IAN Act 2006.

4.2 European Convention on Human Rights

By its nature, the information to be shared under section 36 is likely to be such that article 8(1) of the ECHR is engaged. Article 8 of the ECHR provides:

> "**Right to respect of private and family life**
>
> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society 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 and freedoms of others."

Any such interference must therefore be compatible with article 8(2) of the ECHR. The border agencies are satisfied that any interference is lawful and permissible within article 8(2) for the following reasons.

4.2.1 In accordance with the law

The sharing of information is provided for under section 36 of the IAN Act 2006. The information to which the duty will relate is specified jointly by order by the Secretary of State and the Treasury under that provision (details at Annex C). In this way, the sharing of the data is in accordance with the law for the purposes of article 8(2) of the ECHR.

4.2.2 Legitimate aim

The Secretary of State and the Treasury may only specify information in an order under section 36 of the IAN Act 2006 if satisfied it is likely to be of use for immigration purposes, police purposes or Revenue and Customs purposes and that the nature of the information is such that there are likely to be circumstances in which it can be shared compatibly with the Convention rights. Immigration, police and Revenue and Customs purposes fall within the legitimate aims in Article 8(2) for which proportionate interference with Article 8(1) rights is permitted. In particular:

- the police purpose and the Revenue and Customs purpose of safeguarding national security will be "in the interests of national security" for the purposes of Article 8(2);
- the immigration purposes set out in Annex B will be "in the interests of … the economic wellbeing of the country"; and
- the police, Revenue and Customs and immigration purposes of preventing, detecting, investigating or prosecuting criminal offences will be "for the prevention of disorder or crime" and/or "for the protection of the rights and freedoms of others". (Detection, investigation and prosecution of offences are deemed to have a preventative nature as they reduce the further commission of crime.);
- the Revenue and Customs purposes which relate to
  (a) conduct which is not criminal but which is penalised under legislation and
  (b) information relating to, or provided for purposes connected with, any matter under the care and management of the Commissioners or any assigned matter will be "in the interests of … the economic wellbeing of the country" or "for the protection of the rights and freedoms of others". In addition there may be cases where those purposes also relate to the prevention of disorder or crime even though they do not relate directly to criminal matters.

4.2.3 Proportionate interference

Section 3.3 sets out in more detail the information to be shared by the border agencies. In broad terms, it represents personal data about a person, their travel document, vehicle and journey, freight movements and additional relevant information that the border agencies may hold in respect of the foregoing.

The border agencies are of the view that the sharing of information under section 36 is proportionate to these legitimate aims for the following reasons.

- The sharing of this data will have little tangible impact upon the majority of individuals. The vast majority of persons are of little interest to the border agencies and for them the sharing of this information may facilitate processing at port as access to the information will enable administrative checks to be conducted in advance. The border agencies aim to minimise the impact on the individual through more

efficient capture, selection and analysis in support of targeted intervention delivered through the e-Borders system.

- The sharing will have a greater impact upon the minority who are of interest to the border agencies. However, that interest will be based on a legitimate aim (set out in Article 8(2)) and the interference with that person's article 8 rights which will result from sharing the data will do no more than is necessary to respond to the risk posed by the individual to that legitimate aim.
- The data is necessary for police, immigration and Revenue and Customs purposes as it will enable profiling for those purposes as well as identification and enforcement action for those purposes. Whilst not every element of data will be used in every case of interest, each element of data may be of use in a particular case and it is not possible in advance to determine which elements are relevant to each individual.
- The overall benefits of data sharing are considerable. Access to this information in advance of the arrival or departure of aircraft, ships and trains in or from the UK will enable the border agencies to identify those individuals who are of interest and to mount an appropriate response. As set out above, those responses will prevent crime and disorder, be in the interests of the economic well-being of the United Kingdom and national security and protect the rights and freedoms of others.

4.3 Application of the Data Protection Act 1998

The information to be shared under section 36 of the IAN Act 2006 will (with certain exceptions relating to unaccompanied freight) be information which relates to an individual who can be identified from that data, whether considered in isolation or alongside other data held or likely to come into possession of the border agencies. Therefore the information amounts to 'personal data' for the purposes of the Data Protection Act 1998. In consequence, data sharing under section 36 of the IAN Act 2006 must comply with the terms of that Act.

4.4 Sensitive information

Sensitive personal data is defined in section 2 of the Data Protection Act 1998 as personal data consisting of information as to:

- the racial or ethnic origin of the data subject;
- his political opinions;
- his religious beliefs or other beliefs of a similar nature;
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992;
- his physical or mental health or condition;
- his sexual life;

- the commission or alleged commission by him of any offence; or
- 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.

The data to be shared under section 36 of the IAN Act 2006 includes information acquired under a number of powers specified under that provision as well as information relating to matters in respect of travel or freight specified under that provision. The matters specified in the order made under section 36 cover the behaviour or suspected behaviour of a passenger, member of crew or person involved in the supply chain of a freight movement as well as of an individual connected or possibly connected to such a person. They also cover any action (taken, considered or planned) in relation to any of those persons and their possible connections by the border agencies. Information relating to these matters may include the commission or alleged commission by that passenger of a criminal offence. It may also include information about the passenger's religious beliefs or health. Therefore information shared under section 36 of the IAN Act 2006 may include sensitive personal data.

In addition, the border agencies could receive sensitive personal data direct from carriers under one of the data acquisition powers listed in the order under section 36 of the IAN Act 2006. In particular, the OPI data, which is to be provided only to the extent to which it is known to the carrier, contains free text fields that could include details of a passenger's health under 'general remarks' and could include details of food requests made by a passenger under 'System Service Information' (SSI).

4.5 Eight key data protection principles (DPPs)

Eight key data protection principles (DPPs), which are set out in Schedule 1 to the Data Protection Act 1998, apply to the processing of the data shared under section 36 of the IAN Act 2006. These are considered in turn.

4.5.1 1st DPP: Fair and lawful processing

The first principle requires personal data to be processed fairly and lawfully and, in particular, not to be processed unless:

- at least one of the conditions in Schedule 2 is met; and
- in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

We understand that, in fulfilling its own obligations, under the Data Protection Act 1998, carriers are obliged to provide information to its passengers about the purposes for which data it obtains from passengers will be processed, including the disclosure of such information to Government (where required by law) for border control and wider law enforcement purposes. We will

encourage carriers complying with an obligation to provide passenger information to the border agencies to ensure that the information they provide to their passengers reflects the uses for which information, when disclosed to Government, may be processed.[11] A notice covering how data will be used will also be placed on the e-Borders pages of the Border and Immigration Agency website. Guidance will also be issued to police forces and associated agencies.

It should be noted that the sharing is exempt from the need to be fair and lawful:

- where the disclosure is required by or under any enactment (section 35(1)).

Even where data sharing is exempt by virtue of section 29 and section 35(1) DPA, a condition in Schedules 2 (all data) and 3 (sensitive data) of the DPA needs to be satisfied. The sharing of the information will be necessary for:

(a) the exercise of a function conferred on the border agencies by an enactment (section 36 of the IAN Act 2006); and
(b) the exercise of a function of the Crown, a Minister of the Crown or a government department.

The sharing will therefore comply with paragraph 5(b) and (c) of Schedule 2 and paragraph 7(1)(b) and (c) of Schedule 3 to the Data Protection Act 1998:

> (a) Paragraph 5(b) of Schedule 2 and paragraph 7(1)(b) of Schedule 3 provide for the processing of data for the exercise of any functions conferred on any person by or under and enactment.
>
> (b) Paragraph 5(b) of Schedule 2 and paragraph 7(1)(b) of Schedule 3 provide for the processing of data for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

4.5.2 2nd DPP: Processed compatibly with lawful purposes

The second principle requires personal data to be obtained only for one or more specified and lawful purposes and requires that the data not be further processed in any manner incompatible with that purpose or those purposes.

Much of the information which is to be shared under section 36 will have been acquired under a number of statutory provisions which are specified in an order made under section 36. That information is therefore obtained lawfully. It has also been obtained for immigration, police or HMRC purposes. The remainder of the information to be shared will relate to a matter which is specified in an order made under section 36. That data will have been obtained by a border agency in the course of its functions and therefore for a police, immigration or HMRC purpose.

[11] We will work with carriers to ensure a coherent approach in regard to informing travellers as to what will happen to their personal information.

Data is only required to be shared under section 36 to the extent to which it is likely to be of use for immigration purposes, police purposes or HMRC purposes (section 36(2) of the IAN Act 2006). The border agencies are of the view that processing for any one of those purposes is not incompatible with either of the other purposes. Therefore, the sharing of this data under section 36 will not be incompatible with the purposes for which it was obtained.

It should be noted that the sharing is exempt from principle 2:

- where the disclosure is required by or under any enactment (section 35(1)).

4.5.3 3rd DPP: Adequate, relevant and not excessive data

The third principle requires personal data to be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

All of the personal data to be shared under section 36 relates to passengers and crew entering and leaving the United Kingdom. It is anticipated that this data will initially be requested in respect of certain routes only with a view to covering all routes into and out of the United Kingdom by 2014. All of the data that is specified by order under section 36 of the IAN Act 2006 assists the border agencies in identifying passengers, crew and freight that may be of interest for police, immigration or HMRC purposes. The information is relevant when the subject is involved in the travel process or the investigation relates to the individuals status as a traveller.

To ensure that processing by the border agencies is proportionate, each agency can identify what information is relevant and common data standards will be applied in each joint working arrangement so that the border agencies understand reference codes used. This will aid staff in identifying quickly information that is relevant to them.

The border agencies are satisfied that the sensitive personal data which may be received by and shared between them meets these conditions. For example:

- Medical data is relevant to protecting the health of an individual in respect of whom, an intervention/interception has been/will be made;
- A carrier may provide information on a potentially violent/drunk passenger which will be vital in ensuring the safety of agency staff and the individual in circumstances where an intervention/interception is considered necessary;
- An agency may have historic data on a passenger, for example previous criminal convictions for child trafficking, that may be relevant to another agency; for example, where an individual is identified as making frequent trips with one or more child to whom they are not related.

4.5.4 4th DPP: Accurate and up-to-date data

The fourth principle requires personal data to be accurate and, where necessary, kept up to date.

Data quality standards will be set and agreed with the carrier industry. Where information shared by the border agencies under section 36 is found to be inaccurate, steps will be taken to amend the information and to advise the donor agency and recipient agency of the inaccuracy.

The e-Borders system will monitor data received from the travel industry and use existing information, such as visa information, to confirm the accuracy of the information received. Where appropriate corrections will be made within e-Borders. This will include consultation with the carriers where issues of data quality are identified.

4.5.5 5th DPP: Data not kept for longer than is necessary

The fifth principle requires that personal data not be kept for longer than is necessary for the purpose or purposes for which it is processed.

A key tenet of the data protection principles is the need to ensure that information is retained for no longer than it remains necessary and relevant for the purposes for which it is being processed. Whilst the border agencies have demonstrated that information falling within the scope of section 36 is necessary and relevant for their purposes, they have also identified that such information will not remain so indefinitely. Consequently, each of the border agencies has determined a need to establish data retention periods and controls on access to the information according to continuing need and relevance. These retention periods and access controls are enforced by means of a range of automated and manual processes which are specific to the nature of the information sharing arrangements. The border agencies will review the data retention periods regularly taking into account assessment of business need, factual cases and tangible evidence.
As mentioned in section 2.2, this Code does not cover the processing of data by the border agencies outside the terms of section 36 of the IAN Act 2006.

e-Boc
Data held within the e-Boc is expected to be retained for five years. The system will be set up to ensure that data that has not previously been deleted will be removed upon it being held for five years. This will be done by the e-Borders computer in an automated process. Information may be deleted earlier than the five year retention period following regular audits of the information in the system.
Data will only be transferred from the e-Borders system for the purposes of sharing under section 36 of the IAN Act 2006 when it is necessary for an individual agency to proceed with an investigation. Where data is extracted the retention period would then be governed by the extracting individual agency's data protection policies.

Other joint working arrangements
Where information is shared under section 36 of the IAN Act 2006 outside e-Borders in other joint working arrangements, retention periods are set by the agency providing the data. Sharing in these situations generally involves staff working locally to one another and the sharing is generally through shared access to a computer rather than a physical data transfer. The information will then only be retained on one agency's system and would be retained in line with that agency's data protection and retention policy.

The following sets out the data retention provisions in relation to each border agency

a) Border and Immigration Agency

The Border and Immigration Agency requires the ability to access travel related data for five years, with flexibility to allow access to older data on a case by case basis for a further five years, to support the following key activities:

- Criminal investigations – specialist criminal investigation teams within the Border and Immigration Agency investigate groups and individuals involved in abuse of the immigration system and linked to criminality.
- Analysis of patterns and trends – the intelligence arm of the Border and Immigration Agency analyses patterns and trends on a wide range of data to help detect activity worthy of further investigation or intervention.
- Passenger audit and compliance – data is used as intelligence to identify those who overstay or claim asylum some years after they have arrived. It is also used to confirm a person's previous compliance with conditions of entry and, therefore, inform future risk assessments.

b) UKvisas

UKvisas requires the ability to access travel related data for five years, with flexibility to allow access to older data on a case by case basis for a further five years, (UKvisas issues long-term visas including 5 and 10-year visit visas). This supports the following key activities:

- Ready access to historical data will expedite processing of such visa applications. For example passenger movements and a variety of data recorded by other agencies, will contribute to establishing if repeat applicants have previously complied with the conditions of their visas.

This will directly inform the decisions made by Entry Clearance Officers.

c) The Police

The Police require that data should be retained for as long as it is relevant for 'policing purposes' as specified above.

The Association of Chief Police Officers (ACPO) policy is that all records required for policing purposes will be held for a minimum of six years to meet the requirements of the Limitation Act 1980. Certain categories of data will be retained beyond six years for operational or evidential reasons. Where this is necessary, data will be transferred at the most appropriate time from the e-Borders system and retained in other police systems.

Police have no intention to remove and store traveller data from e-Borders system unless this is necessary for operational or evidential purposes. It is anticipated that most analytical activity will be carried out on the e-Borders system so limiting the amount of data transferred to police systems. Case by case extraction of data will be permitted where it is necessary for intelligence purposes but retention in police systems is not considered routinely necessary or appropriate given the dynamic nature and evidential capability of the e-Borders system. There will be occasions where for operational or evidential purposes retention of limited data sets is necessary. The evidential capability of the e-Borders system allows an accurate evidential trail to be constructed historically. Police guidance advises that statements should only be requested from the e-Borders system where it adds to the evidential trail.

Removal and handling to Police systems will comply with the provisions in the Management of Police Information (MOPI).

d) HM Revenue and Customs

HM Revenue and Customs require travel-related data to be held for as long as it is relevant for Customs purposes. It is estimated that data will need to be retained within the e-Borders system for 5 years, in order to allow appropriate historical analysis of travel data to take place. This is essential in order for HMRC to develop its risk indicators and profiles, which must be flexible in order to respond to changing trends and patterns of criminal behaviour. Where information is required to be removed from the e-Borders system and used as part of an ongoing investigation or prosecution it will be retained in line with current departmental retention requirements which are based on the ACPO policy set out above.

All departments will follow recommendations that come from the review of data handling procedures in Government currently being conducted by the Cabinet Office, which will be published in Spring 2008.

4.5.6 6th DPP: Rights of data subjects including access to personal information

The sixth principle requires personal data to be processed in accordance with the rights of data subjects under the Data Protection Act 1998. There will be

a central point of contact for subject access requests (SAR) in respect of information obtained via e-Boc. Where information in the e-Boc has been enriched by one or more of the agencies the SAR will be forwarded to them for their input. The agencies may hold other information not obtained via e-Boc. This information can be requested from individual agencies - details are at Annex E. It should also be noted that until the central contact point in respect of e-Boc is established (to be in place by summer 2008) SARs must be made to individual border agencies.

There may be exceptional circumstances when the information need not be disclosed in response to a SAR. The Data Protection Act 1998 establishes exemptions from subject access:

- where a third party can be identified from the information, unless the third party's consent has been obtained or it is reasonable in all the circumstances to comply with the request (section 7(4));
- if the exemption is required for the purpose of safeguarding national security (section 28);
- to the extent to which disclosure would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty or of any imposition of a similar nature (section 29); or
- to the extent to which compliance with section 7 would, by revealing evidence of the commission of any offence other than an offence under this Act, expose him to proceedings for that offence (paragraph 11(1) of Schedule 7).

4.5.7 7th DPP: Security of shared information

The seventh principle requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Information will be stored in accordance with published Government Information Assurance guidelines and access restricted according to operational need and legal entitlement.

Whilst the technical and organisational security measures in place at locations where information is shared by the border agencies under section 36 of the IAN Act 2006 will vary depending on the specific operational processes, technical infrastructure and border agency representation, those measures will conform to common standards.

The border agencies take the protection and security of personal data extremely seriously. There are a variety of legislative and internal disciplinary sanctions open to the border agencies in the event that personal data is misused. HMRC and Border and Immigration Agency officers are subject to a penalty of up to two year's imprisonment while police staff are subject to the appropriate sanctions listed at section 5.4.

All staff employed in any joint working arrangement will be subject to security clearance. They will receive appropriate training including training regarding technical, legal and business aspects of the data. Access will be role based and appropriate technical and manual safeguards will be in place to ensure individuals do not access information above their security level. There will be management oversight and regular auditing.

a) e-Borders

In order to protect the data of the individual, the e-Borders system is accredited using Oracle label security. Every user of the system will have access to specific data sets based on their specific profile and security. This will be detailed within the risk assessment and accreditation document set which will be developed as part of the accreditation process.

All actions by users, servers and networks will be audited and collected. The system used will ensure compliance with the provisions of BSI's BIP 0008 and BIP 0009 - Code of Practice for legal admissibility and evidential weight of information stored electronically, especially those records likely to be required as evidence.

In addition all staff are required to read Security Operating Procedures and demonstrate their understanding of these.

Information shared in accordance with this Code will be treated in a manner appropriate to the data's protective marking. Part of the protective marking assessment ensures that the individual's rights are protected in accordance with legislation.

b) Where information is recorded and shared electronically

- Any system will conform to the standards established by ISO/IEC 17799 / BS 7799 or the ISO 27000 series standard.
- Access to the information will be restricted to officers with an appropriate level of security clearance and the system will be capable of preventing access where such clearance is not held or where an officer does not have a legitimate reason for accessing the information.
- The system will be accredited to hold the information at the required protective marking and an appropriate risk management / mitigation plan agreed with the business, data owners and accreditors.
- The system will be capable of auditing access to and use of stored information to an appropriate level.
- The system will be capable of supporting information retention review policy and permit deletion/archiving of information as necessary.
- Where data is transferred to removable media it will be encrypted and subject to security arrangements set by the agency's data protection policies.

c) Where information is recorded and shared manually

- Information will be held in an environment appropriate to its protective marking.
- Access to the information will be restricted to officers who hold an appropriate level of security clearance and who have a legitimate reason for accessing the information.
- Measures will be put in place to ensure that a record is kept of access to stored information and the reasons for this at a level appropriate to its protective marking.
- Measures will be put in place to review retained data in accordance with information retention policy and to delete/archive information as necessary.

The Border Agencies will ensure that the security of data is always top priority. Any additional safeguards that are recommended from the Cabinet Office review will be implemented.

4.5.8 8th DPP: Transfer of data outside the EEA

The eighth principle requires that personal data should 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.

The sharing of data between the border agencies under section 36 of the IAN Act 2006 will involve providing secure links for UK diplomatic missions, including those outside the EEA, to access e-Borders information. This data will be used by entry clearance officers (ECOs) at visa posts overseas when considering visa applications. Principally, e-Borders will provide results of centralised checks of visa applicants against e-Borders watchlists, as well as applicants' previous travel histories (in and out of the UK) where relevant. For example, the e-Boc data may provide evidence of a visa applicant's previous non-compliance with earlier visa conditions. Information will be transferred through secure government systems and will only be accessed on sovereign territory

Data from the e-Boc may be transferred to UK border agency staff operating outside of the EEA in support of their functions. This data will be subject to a high level of protection as it is transmitted only by secure means on across government networks.

As data transferred outside of the EEA will only be done via secure government UK networks, the conditions of the eighth principle are met.

As outlined in section 1, this Code does not cover the sharing of data by the border agencies outside the terms of section 36 of the IAN Act 2006 or its onward dissemination.

Section 5

5.1 Information Access and Control

This section sets out access to information and the sanctions that are to be used for misuse of data.

5.2 Access to information

Access to this information under the e-Borders arrangements will be restricted to those individuals from the agencies that are recruited specifically to work within the e-Boc. Outside the e-BOC, only staff that hold an appropriate level of security clearance and who have a legitimate reason for needing the information shared under section 36 will be able to access it. However, by the very nature of joint-working arrangements it is expected that staff selected to work in these environments will need to access such information. The level of access will be dependent on the role of the individual. Access will be restricted to authorised staff.

5.3 Control and monitoring of information

Access to information will be controlled, monitored and audited through a combination of technical safeguards and operational procedures.

For example, the system will generate reports on police usage and the same approach to supervision of other systems within forces will be used. Randomly selected transactions are followed and officers are challenged to explain the reason for the system's use.

e-Boc managers will be responsible for controlling information received in the operation centre. They will designate access, a list of users will be maintained and reviewed as part of the regulatory process. Currently this is done on a daily basis. Full guidance and training is given as part of the induction process to staff working in the e-Boc.

All joint working systems have a full audit capacity as an integral part. All systems retain activity logs that are subject to audit analysis and integrity checks to ensure compliance with standards**.**

Restrictions in respect of the information that can be shared, strict government standards and the specialist training given to staff engaged in joint working, combined with sanctions for misuse of data, provide high levels of reassurance that personal data will be satisfactorily protected.

5.4 Sanctions for misuse of date

Staff may be subject to the following sanctions in the event of the misuse of data, including its unauthorised or wrongful disclosure:

- Internal disciplinary procedures
- Data Protection Act 1998 (section 55)
- Misconduct and bribery in public offence (enshrined in common law)
- Prevention of Corruption Act 1906
- Official Secrets Act 1989 (section 4)
- Section 19 of the Commissioners for Revenue and Customs Act 2005 (for HMRC staff)
- The UK Borders Bill offence in respect of a Border and Immigration Agency officer who wilfully makes a wrongful disclosure of information, including a wrongful disclosure of Revenue and Customs information.

Section 6

6.1 Procedures for reviewing the code of practice

The Code will come into force on 1st March 2008 in accordance with provision made by order of the Secretary of State and a Treasury Minister. It will be subject to periodic review by these Ministers as required who may revise and reissue the Code as appropriate providing that a draft has been laid before Parliament.

The border agencies will review the Code of Practice regularly, in conjunction with the Information Commissioner's Office (ICO), to take account of: operational or technical developments; further evidence based assessments of the data requirements; changes to procedures; and, to ensure that adequate safeguards are in place to protect data of the individual. The first review will take place six months following the Code coming into force. The review of the Code will be undertaken by a team made up of representatives from each of the border agencies and from the e-Borders Operations Centre.

The Code will also be reviewed in conjunction with the forthcoming report on data handling procedures in Government, conducted by the Cabinet Office which is to be published in the Spring. Recommendations from the report will be used to influence the future direction of data protection and of this Code.

The ICO has been directly consulted during the construction of this Code of Practice and will continue to be engaged throughout the review process. The ICO will be consulted on any significant changes to the Code and will be invited to assess procedures and systems in place in respect of the processing of personal data covered by this Code by each of the border agencies.

Annex A: Section 36 and Section 37 of the Immigration and Nationality Act 2006

36 Duty to share information

(1) This section applies to—

(a) the Secretary of State in so far as he has functions under the Immigration Acts,

(b) a chief officer of police, and

(c) Her Majesty's Revenue and Customs.

(2) The persons specified in subsection (1) shall share information to which subsection (4) applies and which is obtained or held by them in the course of their functions to the extent that the information is likely to be of use for—

(a) immigration purposes,

(b) police purposes, or

(c) Revenue and Customs purposes.

(3) But a chief officer of police in Scotland shall share information under subsection (2) only to the extent that it is likely to be of use for—

(a) immigration purposes,

(b) police purposes, in so far as they are or relate to reserved matters within the meaning of the Scotland Act 1998, or

(c) Revenue and Customs purposes other than the prosecution of crime.

(4) This subsection applies to information which—

(a) is obtained or held in the exercise of a power specified by the Secretary of State and the Treasury jointly by order and relates to—

(i) passengers on a ship or aircraft,

(ii) crew of a ship or aircraft,

(iii) freight on a ship or aircraft, or

(iv) flights or voyages, or

(b) relates to such other matters in respect of travel or freight as the Secretary of State and the Treasury may jointly specify by order.

(5) The Secretary of State and the Treasury may make an order under subsection (4) which has the effect of requiring information to be shared only if satisfied that—

(a) the sharing is likely to be of use for—

(i) immigration purposes,

(ii) police purposes, or

(iii) Revenue and Customs purposes, and

(b) the nature of the information is such that there are likely to be circumstances in which it can be shared under subsection (2) without breaching Convention rights (within the meaning of the Human Rights Act 1998 (c. 42)).

(6) Information shared in accordance with subsection (2)—

(a) shall be made available to each of the persons specified in subsection (1), and

(b) may be used for immigration purposes, police purposes or Revenue and Customs purposes (regardless of its source).

(7) An order under subsection (4) may not specify—

(a) a power of Her Majesty's Revenue and Customs if or in so far as it relates to a matter to which section 7 of the Commissioners for Revenue and Customs Act 2005 (c. 11) (former Inland Revenue matters) applies, or

(b) a matter to which that section applies.

(8) An order under subsection (4)—

(a) shall be made by statutory instrument, and

(b) may not be made unless a draft has been laid before and approved by resolution of each House of Parliament.

(9) In this section—

- "chief officer of police" means—

  (a)in England and Wales, the chief officer of police for a police area specified in section 1 of the Police Act 1996 (c. 16),
  (b)in Scotland, the chief constable of a police force maintained under the Police (Scotland) Act 1967 (c. 77), and
  (c) in Northern Ireland, the chief constable of the Police Service of Northern Ireland,

- "immigration purposes" has the meaning given by section 20(3) of the Immigration and Asylum Act 1999 (c. 33) (disclosure to Secretary of State),
- "police purposes" has the meaning given by section 21(3) of that Act (disclosure by Secretary of State), and
- "Revenue and Customs purposes" means those functions of Her Majesty's Revenue and Customs specified in section 21(6) of that Act.

(10) This section has effect despite any restriction on the purposes for which information may be disclosed or used.

37 Information sharing: code of practice

(1) The Secretary of State and the Treasury shall jointly issue one or more codes of practice about—

(a) the use of information shared in accordance with section 36(2), and

(b) the extent to which, or form or manner in which, shared information is to be made available in accordance with section 36(6).

(2) A code—

(a) shall not be issued unless a draft has been laid before Parliament, and

(b) shall come into force in accordance with provision made by order of the Secretary of State and the Treasury jointly.

(3) The Secretary of State and the Treasury shall jointly from time to time review a code and may revise and re-issue it following a review; and subsection (2) shall apply to a revised code.

(4) An order under subsection (2)—

(a) shall be made by statutory instrument, and

(b) shall be subject to annulment in pursuance of a resolution of either House of Parliament.

Annex B: Legal definition and explanation of 'purposes' for which data will be used

Immigration purposes

"Immigration purposes" is given the same meaning as in section 20(3) of the Immigration and Asylum Act 1999 which defines 'immigration purposes' to mean any of the following

(i) The administration of immigration control under the Immigration Acts ("Immigration Acts" being defined in section 64(2) of the IAN Act 2006);

(ii) The prevention, detection, investigation or prosecution of criminal offences under those Acts;

(iii) The imposition of penalties or charges under Part II of the 1999 Act (carriers liability);

(iv) The provision of support for asylum-seekers and their dependants under Part VI of the 1999 Act (support for asylum-seekers);

(v) Such other purposes as may be specified by order of the Secretary of State. (To date no such order has been made.)

These purposes represent the functions and activities of the Border and Immigration Agency. The Border and Immigration Agency is responsible for managing immigration control in the UK. It is also responsible for considering applications from people who want to work, do business, visit relatives, take a holiday or settle permanently in the UK; dealing with claims for asylum; considering applications for British citizenship and enforcing compliance with the immigration rules.

UKvisas, currently a joint Directorate of the Home Office and Foreign and Commonwealth Office, will be merging with the Border and Immigration Agency as a key element in an integrated approach to border security. UKvisas is responsible for managing the UK's entry clearance (visa) operations. Applications to visit, work and settle in the UK are received at Posts (British Diplomatic Missions (Embassies, High Commissions) and British Consular Posts), where Entry Clearance Officers (ECOs) assess applications against the Immigration Rules, in order to decide whether to issue or refuse visas.

Police purposes

"Police purposes" is given the same meaning as in section 21(3) of the Immigration and Asylum Act 1999 which specifies 'police purposes' to mean the following

(i) The prevention, detection, investigation or prosecution of criminal offences
(ii) Safeguarding national security;
(iii) Such other purposes as may be specified by order of the Secretary of State. (To date no such order has been made.)

In practice the police will use the information for enquiries in connection with:

- the prevention and detection of serious crime;
- the protection of vulnerable victims and witnesses; and
- the execution of warrants and enforcement of other judicial orders.

The information will also be used to:

- identify travellers for intelligence and intervention purposes;
- support intelligence and operational activity; and
- inform on matters regarding the border and deployment of police resources.

HM Revenue and Customs purposes

"Revenue and Customs purposes" mean those functions of Her Majesty's Revenue and Customs which are specified in section 21(6) of the Immigration and Asylum Act 1999. The following functions are specified in section 21(6)

(i) The prevention, detection, investigation or prosecution of criminal offences;
(ii) The prevention, detection or investigation of conduct in respect of which penalties which are not criminal penalties are provided for by or under any enactment;
(iii) The assessment or determination of penalties which are not criminal penalties;
(iv) Checking the accuracy of information relating to, or provided for purposes connected with, any matter under the care and management of the Commissioners or any assigned matter (as defined by section 1(1) of the Customs and Excise Management Act 1979);
(v) Amending or supplementing any such information (where appropriate);
(vi) Legal or other proceedings relating to anything mentioned in paragraphs (i) to (v);
(vii) Safeguarding national security; and
(viii) Such other purposes as may be specified by order of the Secretary of

State. (To date no such order has been made.)

Information shared with HMRC under the IAN provisions will be used to:

- identify individuals or companies involved in the smuggling of, amongst others, Class A drugs, criminal cash, and prohibited or restricted goods such as firearms, offensive weapons, paedophile material and products of animal origin; and
- target smuggling of cigarettes, hand rolling tobacco, alcohol, oils and high-risk counterfeit goods. HMRC's other statutory functions at the border such as the detection of VAT missing trader fraud and the operation of screening equipment to detect illicit movements of nuclear or radiological material will all be supported by access to data shared under section 36.

Annex C: Powers specified in Duty to Share Order made under section 36 IAN Act 2006.

The powers specified in the Duty to Share order are those contained in the following provisions (as applied with modifications to trains arriving and departing the UK via the Channel Tunnel):

- An order made under paragraphs 27(2) of Schedule 2 to the Immigration Act 1971 (power to require provision of information in respect of a ship or an aircraft);
- Paragraph 27B of Schedule 2 to the Immigration Act 1971 (passenger information);
- Paragraph 27(C) of Schedule 2 to the Immigration Act 1971 (notification of non-EEA arrivals on a ship or aircraft);
- Section 35 of the Customs and Excise Management Act 1979 (report inwards) and any directions or regulations made under that provision;
- Section 64 of the Customs and Excise Management Act 1979 (clearance outwards of ships and aircraft) and any directions made under that provision;
- section 77 of the Customs & Excise Management Act 1979 (information in relation to goods imported or exported);
- section 9 of the Commissioners for Revenue and Customs Act 2005 (ancillary powers);
- Articles 181b (entry summary declaration) and 842a (exit summary declaration) and Annex 30A of Regulation (EEC) No. 2454/93;
- section 32 of the Immigration of the Immigration, Asylum and Nationality Act 2006 (passenger and crew information: police powers).

The matters in respect of travel and freight that are specified in the order are the following:

- The behaviour or suspected behaviour of a passenger, member of crew or person involved in the supply chain of a freight movement, whether already undertaken or anticipated, and including any possible

connection with another person held by that passenger, member of crew or person;

- The behaviour or suspected behaviour of a person connected or possibly connected to a passenger, member of crew or person involved in the supply chain of a freight movement, whether already undertaken or anticipated, and including any possible connection with another person held by him;
- Any action taken, considered or planned in relation to a passenger, member of crew, person involved in the supply chain of a freight movement or any person connected or possibly connected to any of those persons by;
  (i) the Secretary of State in so far as he has functions under the Immigration Acts;
  (ii) a chief officer of police; or
  (iii) Her Majesty's Revenue and Customs.

Therefore information in respect of travel and freight that will be shared by the agencies pursuant these specified matters will relate to a passenger or their journey, a member of crew or their journey, or a freight movement and its connected supply chain. This type of information may include details such as:

- previous offences or seizures;
- a passenger's immigration records; and
- other intelligence or information that is valuable to the border agencies in assessing the risk that an individual or freight movement presents to border security.

However, these matters are not specified if or in so far as:

- disclosure of information relating to it may prejudice an investigation or prosecution whether in the United Kingdom or elsewhere;
- the consent of a third party is required for disclosure of information relating to it and that consent has not been obtained;

- disclosure of information relating to it is likely to cause loss of life or serious injury to any person;
- non-disclosure of information relating to it is necessary for the purpose of safeguarding national security; or
- disclosure of information relating to it would be in breach of an obligation of the United Kingdom or Her Majesty's Government under an international or other agreement.

Data would not be shared when if would fall within one of these conditions. Additionally, sub-section 36(7) of the IAN Act 2006 specifically excludes HMRC data collected and held for the former Inland Revenue functions from the duty to share provisions. This means that, for example, sensitive personal tax information will not fall within the duty to share arrangements.

Annex D: List of OPI data[12]

List and description of data elements to be specified by order made under paragraph 27B(10) of Schedule 2 to the Immigration Act 1971

Other passenger information (OPI) data in respect of a passenger that will be provided by the carrier **to the extent that it is known to them.**

- name as it appears on the reservation;
- place of birth;
- issue date of travel document;
- address;
- sex;
- any contact telephone number;
- e-mail address;
- travel status of passenger, which indicates whether reservation is confirmed or provisional and whether the passenger has checked in;
- the number of pieces and description of any baggage carried;
- any documentation provided to the passenger in respect of his baggage;
- date of intended travel;
- ticket number;
- date and place of ticket issue;
- seat number allocated;
- seat number requested;
- check-in time, regardless of method;
- date on which reservation was made;
- identity of any person who made the reservation;
- any travel agent used;
- any other name that appears on the passenger's reservation;
- number of passengers on the same reservation;
- complete travel itinerary for passengers on the same reservation;
- the fact that a reservation in respect of more than one passenger has been divided due to a change in itinerary for one or more but not all of the passengers;
- Code Share Details;
- method of payment used to purchase ticket or make a reservation;
- details of the method of payment used, including the number of any credit, debit or other card used;
- billing address;
- booking reference number, Passenger Name Record Locator or other data locator used by the carrier to locate the passenger within its information system;
- the class of transport reserved;

[12] This annex contains a list of the OPI data to be requested by the Border and Immigration Agency and the police (different elements may be requested by each of those agencies). HMRC will not introduce any requirement for additional data items under the IAN Act 2006.

- the fact that the reservation is in respect of a one-way journey;
- all historical changes to the reservation;
- General Remarks;
- Other Service Information (OSI);
- System Service Information (SSI) and System Service Request information (SSR);
- identity of the individual who checked the passenger in for the voyage or flight or international service;
- Outbound Indicator, which identifies where a passenger is to travel on to from the United Kingdom;
- Inbound Connection Indicator, which identifies where a passenger started his journey before he travels onto the United Kingdom;
- the fact that the passenger is travelling as part of a group;
- the expiry date of any entry clearance held in respect of the United Kingdom;
- card number and type of any frequent flyer or similar scheme used;
- Automated Ticket Fare Quote (ATFQ), which indicates the fare quoted and charged;
- the fact that the passenger is under the age of eighteen and unaccompanied; and
- where the passenger is a person under the age of eighteen and unaccompanied—
    - age;
    - languages spoken;
    - any special instructions provided;
    - the name of any departure agent who will receive instructions regarding the care of the passenger;
    - the name of any transit agent who will receive instructions regarding the care of the passenger;
    - the name of any arrival agent who will receive instructions regarding the care of the passenger;
    - the following details in respect of the guardian on departure—
        - name;
        - address;
        - any contact telephone number; and
        - relationship to passenger; and
    - the following details in respect of the guardian on arrival—
        - name;
        - address;
        - any contact telephone number; and
        - relationship to passenger.

List of data elements to be specified by order made under paragraph 32(5) of the Immigration, Asylum and Nationality Act 2006 (List of data elements required by the Police)

Data for each traveller (and in so far as it applies, whether expressly or otherwise, for a member of crew) to be supplied to the extent that they are known to the carrier;

- name as it appears on the reservation;
- address;
- any contact telephone number;
- fax number;
- e-mail address;
- internet address;
- travel status of passenger or member of crew, which indicates whether reservation is confirmed or provisional and whether the passenger or member of crew has checked in;
- the number of pieces and description of any baggage carried;
- any documentation provided to the passenger or member of crew in respect of baggage;
- ticket number;
- date and place of ticket issue;
- seat number allocated;
- seat number requested;
- check-in time, regardless of method;
- date on which reservation was made;
- identity of any person who made the reservation;
- any other name that appears on the passenger's or member of crew's reservation;
- the fact that a reservation in respect of more than one passenger has been divided due to a change in itinerary for one or more but not all of the passengers or members of crew;
- Code Share Details;
- method of payment used to purchase ticket or make reservation;
- details of the method of payment used, including the number of any credit, debit or other card used;
- Passenger Name Record Locator or other data locator used by the carrier to locate the passenger or member of crew within its information system;
- the name, address and contact details of the passenger's or member of crew's sponsor in the United Kingdom;
- the fact that the passenger is under the age of eighteen and unaccompanied;
- the fact that the passenger is under the age of eighteen and travelling with a person who has not declared himself to be a family member; and
- name and contact details of an adult dropping off an unaccompanied passenger under the age of eighteen at a port or station.

Annex E: Subject Access Request Information

Agency	Information Required	Address	Further information
Border and Immigration Agency	Requests must be made in writing and must be accompanied by payment of a £10 fee.	The Data Protection Unit Lunar House 40 Wellesley Road Croydon CR9 2BY	The Border and Immigration Agency details its arrangements for receiving and processing Subject Access Requests (SAR) in Chapter 24 of the Immigration Directorates' Instructions, which are published on the Border and Immigration Website at www.ind.homeoffice.gov.uk.
UKVisas	Requests must be in writing (this includes emails as well as letters and faxes). Written requests must be accompanied by two forms of identification, to ensure that personal data is only released to the person to whom the data is relevant.	Information Rights Team Information Management Group Foreign and Commonwealth Office Old Admiralty Building London SW1A 2PA Tel: + 44 (020) 7008 0123 E-mail: dp-foi.img@fco.gov.uk	UKvisas' arrangements for handling Subject Access Requests are detailed in the *Access to Information Section* of the Foreign and Commonwealth Office website at http://www.fco.gov.uk
HM Revenue and Customs	Requests must be in writing. Requests must included the type of information required, name, address, date of birth and any accompanying information such as National Insurance Number, tax reference or VAT number.	HM Revenue & Customs, Data Protection Subject Access Unit, Room BP5001, Benton Park View, Longbenton, Newcastle upon Tyne NE98 1ZZ.	HMRC have set out their policy for providing this free service on the HMRC web site in a fact sheet at: http://www.hmrc.gov.uk/leaflets/data_prot_factsheet.pdf

Police	An individual can also go to any police station and the request will be forwarded to the relevant force.		The various police forces have published guidance on how individuals can make subject access requests.

Annex F: Glossary of terms

Travel Document Information (TDI)	TDI refers to a passenger's or crew member's biographic and travel document details, normally contained in the machine-readable zone of a passport or other travel document.
Other Passenger Information (OPI)	OPI refers to information held by a carrier in connection with a passenger's booking or reservation.
Service Information (SI)	SI is information related to the flight, train or ship the passenger or crew member is travelling on.
Vehicle Registration Mark (VRM)	VRM is the registration mark on a vehicle or trailer.
e-Borders	e-Borders is the border agencies' strategic IT solution to the need for acquisition and joint pooling and analysis of electronic passenger information.
e-Borders Operation Centre (e-BOC)	The e-BOC will be jointly operated by the border control agencies. Data provide by carriers will be analyised, acted upon and disseminated as necessary.
IAN Act 2006	Immigration, Asylum and Nationality Act 2006.
Section 36 IAN Act 2006	Introduced a requirement for the Secretary of State (in so far as he has functions under the Immigration Acts), Her Majesty's Revenue & Customs and a chief officer of police ("the border agencies") to share passenger, crew, freight, service and other travel related information where the information is likely to be of use for immigration, police or Revenue and Customs purposes.
Section 37 IAN Act 2006	Introduced a requirement that the Secretary of State and the Treasury shall issue one or more codes of pratice about the use of information shared in accordance with section 36 and the extent to which, or form or manner in which, shared information is to be made available in accoradance with that section.