

Deputy Chief Executive

[Redacted contact details]

[Redacted contact details]

[Redacted contact details]

[Redacted contact details]

Tel [Redacted contact details]

Email [Redacted contact details]

Web www.ukba.homeoffice.gov.uk

24 August 2009

Mr Jonathan Faull
DG Justice, Liberty and Security
European Commission

Dear Jonathan

UK e-Borders system

Thank you for taking the time to discuss the UK's e-Borders scheme with me on 16 July and for your letter of 27 July to Julie Gillis, the programme director. I found the discussion very helpful and undertook to provide further information on some of the issues you raised. I am also attaching to this letter (at **Annex A**) our response to the supplementary questions forwarded by the Commission following the meeting between delegates from the UK and the Commission Heads of Department on 23 June. I am more than happy to discuss any of this with you or your colleagues in whatever way is most useful.

I would like to assure you that it remains our firm view that our e-Borders scheme is compatible with the EC Directives on Free Movement of Persons and Data Protection.

On free movement, we can confirm categorically that carriers will not be asked to deny boarding to EU citizens or their family members as a result of data received under e-Borders. As is currently the case, the right of such persons to be admitted to the UK will be assessed by an immigration officer at our border controls. Admission will only be refused in accordance with Directive 2004/38/EC and the rights set out in Chapter VI of the Directive will be respected. The advantage of e-borders is that immigration officers will have advanced warning of the person's arrival and as a result should be able to deal with the case more efficiently. This better targeted approach will facilitate more efficient and quicker processing for the vast majority of passengers.

In relation to data protection, we have a clear legislative basis in both primary and secondary UK law for the collection and processing of this data. The legislation has been properly scrutinised by the UK Parliament and we consulted the UK's Information Commissioner during the drafting of the law. In our view this is both proportionate and necessary to fulfil one of the legitimate interests of society i.e. protection of our border. As we said in our response to Pilot Complaint 348/09/JLSE,

a safer UK means a safer European Union. The scheme is compatible with the UK Data Protection Act 1998 which transposes the Data Protection Directive.

You mentioned certain key principles on which the Commission will want to be assured. Whilst these points are covered in more detail in our original response ([Pilot Complaint 348/09/JLSE](#)) and in our response to the Commission's supplementary questions (**Annex A**) I thought it would be helpful to summarise the e-Borders position on these points:

- **It is clear to those travelling that their personal data is collected by carriers for e-Borders purposes**

We are committed to being transparent about what information will be collected on travellers and how that information will be used. Notwithstanding that the UK e-Borders system does not collect data directly from passengers, but from carriers, we engage very closely with the carrier community to ensure that carriers have the most up to date information about the UK's e-Borders system that can be passed on to passengers, including what data is being collected and why. This is most commonly done through the internet sites of the majority of carriers, the internet increasingly being the primary method of arrangement for travel (and purchasing of tickets) for those entering and departing the UK. We are providing carriers with a clear statement on the purposes of this data which they may want to use on their websites.

In addition to this, information that details what data is collected by e-Borders and why, is available to the public on the UK Border Agency website (see below for more detail).

It is also worth making the point that as an ever-increasing number of countries across the globe are collecting passenger information for those crossing their borders, an increasing number of carriers (primarily in the international aviation sector) have decided to make the provision of API data (by the passenger) a condition of carriage. This will be reflected in the terms and conditions between carrier and passenger.

Whilst our approach to date has been heavily influenced by the airline industry, as we now begin to roll-out e-Borders to the cross-border rail and international maritime industries, we will work as closely with them to find solutions that are most suitable. Finally, and in this context, I would make the point that the UK would like to see (and is actively working towards) a common EU protocol regarding how and when passengers are informed (through the agreement of an EU Framework Decision on Passenger Name Records).

- **We should be clear on what data we are collecting and for what purposes**

Data received by e-Borders will be used to secure our border from the threats of international terrorism, crime, and illegal immigration. We are clear what information will be collected on travellers and how that information will be used. The detail concerning this information is available to the public on the UK Border Agency website. The website explains that the data from the machine readable

zone of a passport: will be collected on all passengers (Names, nationality, date of birth, gender, document number and type, and expiry date) or the relevant equivalent data from the identification relied upon to travel. In addition it gives details of how data related to bookings and reservations (Other Passenger Information) will be collected on some routes on a risk basis. The website provides straightforward examples of the practical use of the data collected by e-Borders:

- **It is clear who will have access to the data collected by e-Borders**

Data collected by e-Borders is only available to trained operators within the UK Joint Border Operations Centre (JBOC), who have a high level of security clearance and are subject to stringent audit requirements.

Data is kept securely and can only be transferred outside the European Economic Area in accordance with domestic, European and international law including the Data Protection Directive and over-arching EU – third country agreements such as those between the EU and Australia, Canada and the US.

- **It is clear how long the data will be kept**

Data is currently retained for a maximum of ten years by e-Borders, five years in an active database followed by five years in an archived database and this is clearly stated on the UK Border Agency website. The Commission will be aware that when it published its Commission Staff Working Document accompanying the proposal for the PNR Framework Decision in 2007 that it proposed a retention period, in respect of PNR data, of five years in an active database followed by eight years in an archived database¹. The e-Borders Code of Practice, which was published in 2008, followed the Commission proposal but instead opted for a lesser period of 5 years active and 5 years archived. Once the data is archived, it can only be accessed on a case by case basis for specific reasons. As mentioned at the meeting with Commission representatives in June, the UK will act consistently with practices to be adopted within the EU and the UK will adapt its retention periods in order to comply with the draft Framework Decision on Passenger Name Records as and when this is agreed.

- **The travelling public have appropriate information about how they can access data held on them and seek correction of any mistakes**

Any individual can make a subject access request to the relevant organisation under the Data Protection Act 1998 to see the information which is held on them, and to correct any inaccurate data held. Contact details on to whom those applications can be made are set out in an annex to the Code of Practice referred to above and details are also available on the UKBA, HMRC, and Police forces public websites. It is intended that a single point of contact will be established to facilitate subject access requests regarding data held on e-Borders. We will be

¹ The document states that “this period was deemed as striking an acceptable balance between what the law enforcement authorities wanted and what is considered adequate and acceptable.”

more than happy for the Commission to input into the development of this process.

Individuals also have the right to make enquiries about e-Borders under the Freedom of Information Act.

During our call you asked some specific questions which I would like to address below. Firstly, you asked what would happen if the US asked for information from the e-Borders database. There is a Memorandum of Understanding between the UK Joint Border Operations Centre (JBOC) and the US National Targeting Centre. However, this is primarily to facilitate operational co-operation and sharing of data on a specific and case by case basis. It does not provide for the bulk transfer of personal data nor direct access to the database by US authorities. The US is committed to abiding by similar levels of data protection in respect of the data which may be sent from the UK, following a request made under the MOU, as are set out in the EU – US PNR Agreement. That Agreement deems the US Department of Homeland Security to have adequate levels of protection for PNR data transferred from the EU. Further, any data shared would, of course, be in accordance with the UK Data Protection Act 1998, which transposes the Data Protection Directive 95/46/EC. Finally, you will already be aware that the UK has taken a very active role in working to secure a common platform at EU level on the collection, use and sharing of (including with third countries) PNR data through the development of an EU PNR Framework Decision.

Secondly, you also asked about our plans for the implementation of e-Borders on routes between the UK and Ireland in light of our inability to secure amendments to our domestic legislation regarding control of the Common Travel Area (CTA). The national legislation that underpins e-Borders does not discriminate according to route, allowing the UK Border Agency, the police or Her Majesty's Customs and Revenue to request passenger and crew data on all sea, air and rail routes to and from the UK, including on journeys between Ireland and the UK. The e-Borders programme is on a staged roll out to different countries, transport sectors and routes and it has not yet been rolled out to cover journeys between Ireland and the UK. However, our intention remains that e-Borders will cover air and Sea routes between the UK and Ireland.

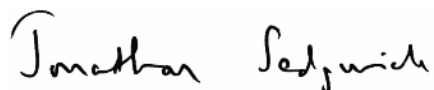
The proposed legislative changes to the CTA would have given us powers to more regularly control immigration at the points of entry into the UK from the rest of the CTA. However, this would have been *in addition* to the powers we already have that allow us to implement e-Borders and as such, its absence does not prevent implementation of e-Borders on this route.

Thirdly, you asked about people in transit from, say, Germany via Heathrow to US who were staying airside. As set out above, the legislation enables relevant officers to require carriers to provide the UK border authorities with passenger and crew data on journeys arriving in or leaving the UK. This includes transit flights as there is no requirement for the individual to have entered the UK. However, the fact that a passenger was transiting the UK and not planning to enter would inform our decision on whether or not to issue an alert to the relevant agency and/or intervene should a hit occur against our watchlist. Our approach would be very much on an individual, case by case basis and proportionate to the perceived level of risk.

Finally, you asked whether there were situations where people travelled without giving any personal details - for example someone turning up at the last minute as a passenger for a cross-channel ferry. Whilst it is covered in greater detail in the formal response, the key point here is that while it is very much our intention that e-Border's will cover these routes into and out of the UK, we are still finalising how e-Borders will be applied to the maritime and cross border rail industries. As we have previously advised the Commission and as set out above, the e-Borders programme has a staged roll out. The effect of this is that the requirement to provide relevant data to the programme is being applied to particular carriers on particular routes. Accordingly, our engagement with the airline carriers has been more advanced than with carriers in other transport sectors.

It is correct that there is further to go regarding international maritime and cross border rail carriers as they, unlike airline carriers, do not currently have booking systems which so closely support the e-borders process in the way that air carriers do. We are working very closely with both industries to develop processes which fit these modes of transport. We would very much welcome the close engagement of the Commission on this too.

Yours,



JONATHAN SEDGWICK

ANNEX A

EU PILOT COMPLAINT 348/09/JLSE

CONCERNING THE UK E-BORDERS SCHEME:

RESPONSE TO SUPPLEMENTARY QUESTIONS ON

**FREE MOVEMENT OF EU CITIZENS AND THEIR FAMILY MEMBERS
AND TO DATA PROTECTION ASPECTS**

(A) FREE MOVEMENT OF EU CITIZENS AND THEIR FAMILY MEMBERS

1. Denial of entry by carriers: could the UK authorities confirm that carriers would not be asked to deny boarding to EU citizens or their family members on any grounds?

1. We can confirm that carriers will not be asked to deny boarding to EU citizens or their family members as a result of data received under e-borders. As is currently the

case, the right of such persons to be admitted to the UK will be assessed by an immigration officer at our border controls. Admission will only be refused in accordance with Directive 2004/38/EC and the rights set out in Chapter VI of the Directive will be respected. The advantage of e-borders is that immigration officers will have advanced warning of the person's arrival and as a result should be able to deal with the case more efficiently.

2. Sanctions: could the UK authorities confirm that they would not enforce sanctions against carriers which do not provide the requested data due to no fault on their part (e.g. where the EU citizen does not provide the data or the carriers are not authorised to collect and transfer the data)?

2. Yes, we can confirm this. The overall intention is that sanctions are aimed at carriers who do not cooperate with e-borders and carriers who have in place systems to collect data will not need to fear prosecution where they are prevented from supplying data in an individual case due to no fault on their part. Further, in all cases there is a statutory defence available to a carrier of having a reasonable excuse for failing to comply with a request to provide data (which is set out in section 27(2)(b)(iv) Immigration Act 1971 as amended in respect of a request made by an immigration officer and section 34(1) Immigration, Nationality and Asylum Act 2006 made by a police officer).

3. Availability and collection of data: Could the UK authorities confirm this? (That an EU national will not be refused entry on the basis that their passenger data is unavailable to the border control officer for whatever reason).

3. Yes, we can confirm this. Provision of data in advance is absolutely not a condition for EU citizens and their family members to exercise their right to free movement. As confirmed in the UK's first response to the Commission pilot complaint at paragraphs 29 and 31 respectively:

“29. More generally, the right of EU citizens to enter the UK with a valid identity card, passport or to prove by other means their right of free movement, as required by Article 5(1) and (4) of Directive 2004/38, is set out in UK law in regulation 11 of the Immigration (European Economic Area) Regulations 2006 No. 1003. The UK's border authorities check the documents presented on the arrival of EU citizens at the UK's border crossing points. [...]

31. EU passengers to the UK will not be required to carry any additional documentation as evidence of their free movement right other than that as required by the Directive. Their right to enter or leave the UK under the conditions set out in Articles 4 and 5 of the Directive is not affected.”

(B) DATA PROTECTION

1. Legal basis for the collection and processing of personal data by carriers in the Member State of departure.

(a) What is the legal basis on which carriers would lawfully collect in the Member State of departure personal data required by the UK e-Borders legislation and lawfully transfer them to the UK authorities?

4. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('the Data Protection Directive') as transposed in the national legislation of that other Member State applies to the personal data concerned here.

5. However, the wording of this question assumes that the relevant passenger data will always only be located in the Member State of departure, and that the request for the passenger data will always be made by the UK border authorities to the division of the carrier that is based in the Member State of departure. Neither of these assumptions is correct. E-Borders is designed to work on a flexible basis as to where it obtains the information. The information may be provided from the departure country, or from UK based element of the carrier, or indeed from a body of the carrier based in a third country if the carrier wishes.

6. Consequently two points arise. Firstly, it is important to determine which organisation is the data controller in respect of the relevant passenger data and where that organisation is located in order to determine which national data protection legislation applies. Secondly, it is necessary to identify all the locations where the carrier processes the relevant passenger data being requested. For example an Irish airline may operate a flight between the UK and France. Because it has check-in desks in airports of both states it will process personal data in both the UK and France, and so is a data controller in both jurisdictions. National legislation requires air carriers operating flights into and out of the UK, to provide relevant data about a flight when requested to do so by the relevant agency in the UK. If the carrier receives and processes personal data in the UK it will be subject to the UK Data Protection Act 1998 which provides that (at section 5):

*“(1) ... this Act applies to a data controller in respect of any data only if—
(a) the data controller is established in the United Kingdom and the data are processed in the context of that establishment, [...]*

(3) For the purposes of subsections (1) and (2), each of the following is to be treated as established in the United Kingdom—

(a) an individual who is ordinarily resident in the United Kingdom,

(b) a body incorporated under the law of, or of any part of, the United Kingdom,

(c) a partnership or other unincorporated association formed under the law of any part of the United Kingdom, and

(d) any person who does not fall within paragraph (a), (b) or (c) but maintains in the United Kingdom—

*(i) an office, branch or agency through which he carries on any activity,
or*

(ii) a regular practice; [...].”

7. This is consistent with the terms of Article 4 of the Data Protection Directive, taken together with recital (19) of the Directive, which provides that when the same

data controller is established on the territory of several Member States, it must take the necessary measures to ensure that each of the establishments complies with the obligations laid down by the national law applicable. Thus in practice because carriers have offices, branches or agencies in all of their destinations as a matter of commercial necessity to check in and process passengers and their luggage, they are obliged to comply with the national law of each member state they operate in.

8. An air carrier operating flights into and from the UK receives and processes personal data from passengers, where this personal data is entirely processed or concurrently processed in the UK (such as where the booking system is located in the UK or where the carrier has an office in the UK handling passenger lists and other administration) the requirement to provide such data to the e-Borders system when requested amounts to a UK legal obligation made in accordance with the provisions of the Data Protection Act 1998, which is the UK implementation of the Data Protection Directive.

9. In respect of personal data relating to flights to or from the UK, which the carrier may not process in the UK and which may therefore not fall within the scope of the UK Data Protection Act 1998 but is held and processed in another Member State where the carrier is a data controller in respect of passenger data, then the application of the data protection legislation applicable in that Member State becomes relevant. As set out in the UK's first response at paragraph 26, "... to the extent that any carrier has raised issues about the application of data protection law, the e-Borders programme has been working with them and the data protection authorities in other Member States to reach amicable and practical solutions. Such engagement will continue."

10. The Commission notes that Directive 2004/82/EC on the obligation of carriers to communicate passenger data ('the API Directive') cannot constitute a Community legal basis for the collection and transfer of personal data of passengers on intra-EU flights to the UK. However, recital 8 to that Directive specifically records the "... freedom of the Member States to retain or introduce additional obligations for air carriers or some categories of other carriers, ..., whether referred to in this Directive or not ..." without prejudice to the provisions of the Data Protection Directive. In addition, recital 12 records that "... it would be legitimate to process the passenger data transmitted for the performance of border checks also for the purposes of allowing their use as evidence in proceedings aiming at the enforcement of the laws and regulations on entry and immigration, including their provisions on the protection of public policy (ordre public) and national security, ...". The UK's position is that the scheme is compatible with the Data Protection Directive for the reasons set out below.

11. Article 7 of the Data Protection Directive sets out the circumstances in which personal data may be processed and these will apply to the transfer of that data to e-Borders. Article 7(c) provides that the data may be processed where it "... is necessary for compliance with a legal obligation to which the controller is subject;". If the carrier is a controller established in the UK then the legal obligation is that which arises from UK legislation. This is explained in paragraph 8 above. Indeed, in accordance with Article 18 of the Data Protection Directive, many carriers have registered with the UK Information Commissioner's Office as a data controller in the

UK in respect of the processing of passenger data. For example, Air France, Alitalia, Iberia, Brittany Ferries operating as BAI (UK) Limited, Eurostar (UK) Limited and Eurostar Group Limited are all registered in the UK².

12. However, this reference is not necessarily confined to a legal obligation which arises in the national law of the state of the data controller. This will particularly be the case if the carrier is established in more than one Member State (see Article 4(1)(a) Data Protection Directive). The obligation may also arise from a legal obligation affecting it in another Member State in which it operates its business – in this case the UK, for carriers operating to and from the UK.

13. In addition, the same result may arise with the application of Article 7(f) of that Directive which provides that personal data may be processed when it "... is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)."

14. The UK considers that collection of data through the e-Borders programme pursues a legitimate interest and the UK border authorities (the UK Border Agency, police or customs) are the third party to whom the data would be disclosed by the carrier and these are the authorities who pursue that interest. The interest is in stronger security and better efficiency in border control particularly for immigration, police, customs and related statistical purposes. The legitimate interest in collecting advanced passenger information from carriers has been accepted, in principle, by the Community legislature in Directive 2004/82/EC on the obligation of carriers to communicate passenger data³. A stronger UK border is also a stronger border for the EU generally and those carriers operating into and out of the Schengen area. The UK (and Ireland) has the right, under Article 1 of the Frontiers' Protocol⁴ to exercise, at its frontiers with other Member States, controls on persons seeking to enter.

² The Information Commissioner's Office register of data controllers in the UK for the purposes of the UK Data Protection Act 1998 can be found at: <http://www.ico.gov.uk/ESDWebPages/search.asp>

³ Recital (8) of Directive 2004/82/EC of 24 April 2004 on the obligation of carriers to communicate passenger data provides that its provisions may be extended by Member States to include additional obligations or to other carriers. Further, recital (12) provides that in accordance with Directive 95/46/EC, '... it would be legitimate to process the passenger data transmitted [pursuant to the Directive] for the performance of border checks also for the purposes of allowing their use as evidence in proceedings aiming at the enforcement of law and regulations on entry and immigration, including their provisions on the protection of public policy (order public) and national security, any further processing in a way incompatible with those purposes would run counter to the principle set out in Article 6(1)(b) of Directive 95/46/EC.'

⁴ Protocol on the Application of Certain Aspects of article 14 of the Treaty Establishing the European Community to the United Kingdom and Ireland (as annexed to the Treaty on European Union and to the Treaty establishing the European Community).

15. In addition, the Convention on International Civil Aviation (1944) (otherwise known as the Chicago Convention)⁵ establishes certain standards with which contracting States⁶ and carriers operating in their jurisdiction are expected to comply. For instance, this includes a provision that every aircraft shall carry a number of documents in respect of their passengers, including a list of their names and their place of embarkation and destination.⁷ It also anticipates the principle of collecting information about passengers in advance of travel⁸.

16. Accordingly, the UK has the right under EC law to check travel document information of persons seeking to enter under the Frontiers' Protocol. Air carriers are already collecting this information (also known as advanced passenger information) from passengers. The UK is simply seeking this information which has already been provided to the carrier albeit at an earlier point before arrival in or departure from the UK for the legitimate purposes of border control. The UK is of the view that this is compatible with an individual's rights and freedoms provided for under the Data Protection Directive for the purposes of Article 7(f)⁹.

17. Since Article 7(f) required transposition into national legislation of all Member States, it would provide, in the view of the United Kingdom, a basis to permit carriers who are data controllers established in other Member States and who hold the relevant passenger data in those States to provide any data held there and not in anyway processed in the UK (and thus not subject to the UK Data Protection Act) to e-Borders in compliance with that national legislation that implements Article 7(f).

18. A similar point arises in respect of Article 7(e) which states that Member States shall provide that personal data may be processed only if "... processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed".

19. For the purposes of Article 7(e), the United Kingdom is of the opinion that the collection of passenger data by e-Borders is in the public interest, particularly for the reasons set out in paragraph 14 above. The United Kingdom, the Member State in which the carrier is established as a data controller and the EU more generally have a public interest in the security of the border. In which case, the transfer of data by a carrier to e-Borders would be necessary for the performance of a task carried out in

⁵ The Convention can be found at: http://www.icao.int/icaonet/dcs/7300_cons.pdf and Annex 9 on Facilitation found at: http://www.parlament.hu/irom/02918/fugg/en/an09_cons.pdf

⁶ Ireland, the UK and all other EU Member States are Contracting States.

⁷ See Article 29(f).

⁸ See section 3.47 to Annex 9 (Facilitation) to the Convention.

⁹ As set out the original response to the Commission, there is a published Statutory Code of Practice which provides an analysis of the compliance of the data sharing provisions of e-Borders with the UK Data Protection Act 1998 and Article 8 European Convention on Human Rights.

the public interest and, also, in the exercise of the official authority vested in the UK border authorities to whom the data would be disclosed.

20. The United Kingdom also recalls that one of the objectives of the Directive, as set out in Article 1(2), is that “Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1 [protection of personal data].” The Data Protection Directive is a harmonising directive that seeks to establish common protection across the EU for personal data in order to give effect to the common market by allowing the free flow of data between Member States through the provision of safeguards common to all Member States. The United Kingdom also notes that Recital 5 envisages “a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic or social activity in member states;” and that Recital 8 refers to removing obstacles to flows of personal data, and the level of protection of the rights and freedoms of individuals with regard to the processing of such data being equivalent in each member state. The United Kingdom is of the opinion that the e-Borders scheme is consistent with the data-sharing activity envisaged by, and supported by the common standards expressed in, the Data Protection Directive.

21. Additionally, the personal data that is proposed to be processed as a part of e-borders applying to intra-EU travel is no different to that routinely being required and obtained by carriers based in Member States in relation to travel to states outside of the application of the Data Protection Directive. As the UK delegation mentioned in the meeting with Commission representatives in June, several third countries outside the EU including the USA, Canada, Mexico, China, Japan, Antigua, Barbados, Grenada, Jamaica, St. Lucia, Trinidad & Tobago, India, Australia, New Zealand and the Republic of Korea are collecting passenger data from EU carriers on journeys between EU Member States and the States concerned. It would therefore be perverse and contrary to the purpose of the Data Protection Directive if the collection and transfer of this data can be done legitimately on routes external to the EU but is prohibited when the routes fall wholly within the EU and its area of common data protection in respect of which the UK fully complies.

22. Accordingly, the United Kingdom considers that these provisions demonstrate the compatibility of the e-Borders programme with the Data Protection Directive. Further, since this Directive has been transposed in the national legislation of each Member State, the United Kingdom considers that the application of these provisions provide an appropriate legal base for a carrier to provide passenger data to the UK border authorities under the legislation creating the e-Borders programme.

(b) Does UK legislation require the collection of data which is additional to that normally collected by carriers – in other words personal data that carriers would not collect but for the legislation?

23. As the Commission acknowledge in the text of the original complaint, the information which can be requested from a carrier by an immigration or police officer is specified in UK legislation – the Immigration and Police (Passenger, Crew and

Service Information) Order 2008 (No. 5) ('the 2008 Order')¹⁰. However, for the Commission's information the list of data elements is replicated in Annexes 1 - 4 to this response. The effect of the 2008 Order is that the carriers, when requested to do so, must provide the passenger's Travel Document Information (TDI) which is also known as Advance Passenger Information (API) which is contained in the machine readable zone (MRZ) of the passport. Further, in order to ensure compatibility with EC law on the free movement of persons and Directive 2004/38/EC in particular, it provides that where a travel document is not presented for travel, then the carrier should provide information in respect of the identification relied upon. The list of the data which can be required and is mandatory for the carrier to provide is set out in Annex 1, in respect of a request made by an immigration officer, and Annex 3 in respect of a request made by a police officer. The UK considers the collection of this type of data is necessary and proportionate to the immigration, police and customs purposes pursued by the respective UK border agencies.

24. Other Passenger Information (OPI) or Passenger Name Records (PNR) as it is known in the airline industry will only be requested on specific routes and, importantly, it could only be mandatory for the carrier to provide the requested information to the extent the carrier has that information. The carrier could not be required to collect the data if it has not already collected it for its own purposes. This is set out in the national legislation (the 2008 Order). The list of OPI data which could be requested, by an immigration officer, can be found in Annex 2, and OPI data which can be requested by a police officer can be found in Annex 4. There is no intention to make the collection of PNR data mandatory unless or until this is required by the draft EU Framework Decision on PNR which is currently being negotiated. You will already be aware that the UK has taken a very active role in working to secure a common platform at EU level on the collection, use and sharing of (including with third countries) PNR data through the development of an EU PNR Framework Decision.

25. Air carriers routinely collect travel document information in respect of their passengers because of legal obligations which govern this transport sector. As set out above, it is also relevant to note the international legal context in which air carriers operate including the Chicago Convention¹¹ which sets standards as to the passenger information which air carriers should hold, including as to how advanced passenger information may be collected.

26. In respect of maritime carriers operating on routes between the UK and other Member States, the UK's original response to the Pilot Complaint 348/09/JLSE records as follows:

“32. The Commission may also note that the requirement for passengers to provide certain information in advance of travel to maritime passenger

¹⁰ This can be found on the Government legislation website at: http://www.opsi.gov.uk/si/si2008/pdf/ukxi_20080005_en.pdf

¹¹ The Convention can be found at: http://www.icao.int/icao/net/dcs/7300_cons.pdf and Annex 9 on Facilitation found at: http://www.parlament.hu/irom/02918/fugg/en/an09_cons.pdf

carriers in advance of travel on intra-EU routes already exists in Community legislation and the United Kingdom is not aware that this has affected the exercise of free movement rights of EU citizens. Article 5 of Directive 98/41/EC requires the collection of the information before departure and that this is transmitted to a designated place on shore within 30 minutes of departure.”

27. In any event, as we have previously advised the Commission and as set out above, the e-Borders programme has a staged roll out. The effect of this is that the requirement to provide relevant data to the programme is being applied to particular carriers on particular routes. Accordingly, our engagement with the airline carriers has been more advanced than with carriers in other transport sectors.

28. It is correct that there is further to go regarding maritime and cross-border rail carriers as they, unlike airline carriers, do not currently have booking systems which so closely support the e-borders process in the way that air carriers do. We are working closely with the international maritime and cross border rail industries to develop processes which fit these modes of transport, recognising firstly that vehicles rather than individual passengers are the main transactional unit for the maritime industry and a sizable proportion of the cross-border rail industry and secondly that industry requirements on the maritime and rail sector are less onerous than those on the aviation sector in terms of data which is already collected. Our current thinking is that the travel document information could be linked to the vehicle registration mark and automatic number plate recognition used to facilitate swifter passage through the port. As we continue to finalise how e-Borders will be applied to the maritime and cross border rail industries, we welcome the close engagement of the Commission on this.

2. Data quality and proportionality

(a) What kind and number of personal data will be processed and will citizens be required to communicate all the personal data laid down in UK legislation?

29. The requirement made by an immigration or police officer to provide data on passengers to e-Borders is to the carriers and not, directly, to the passenger. The UK refers you to the answer to data protection question 1(b) above regarding the kind and number of personal data which may be processed.

(b) What would be the consequences for an individual who refuses to disclose his / her personal data to a carrier?

30. We refer you to the answers given above to the free movement of persons' questions one and three.

31. In addition, section 34 of the Immigration Nationality and Asylum Act 2006 makes it an offence for a passenger or member of crew who does not comply with a requirement to provide to the owner or agent of a ship or aircraft any information that he requires for the purpose of complying with a requirement imposed by the police to provide passenger or service information. There was one prosecution under this offence in 2007, the last full year for which figures are published and it is not

currently known whether this was of a carrier or an individual. This power is used sparingly for police purposes/crime prevention and counter-terrorism purposes. This is underlined by the fact that there is no equivalent offence for a passenger or crew member failing to provide information related to a request made by an immigration officer. Significantly, it is subject to a statutory defence for the passenger of reasonable excuse for failing to comply with a request. The UK would not wish to rule out the possibility of police requesting information on an EU national, but such a request would be in the vast majority of cases in the context of a criminal investigation or designed to identify those who were wanted on European Arrest Warrant, for instance, or to whom a travel ban applied or who were considered to be a threat to national security.

(c) Should carriers be required, directly or indirectly (e.g. by fines) to collect all the personal data laid down in UK legislation?

32. We refer you to the answer to question two on the free movement of persons.

(d) Will carriers to whom individuals have declined to give the data be denied from boarding by carriers and so indirectly prohibited from entering the UK?

33. We refer you to the answer to question one on the free movement of persons.

(e) Will carriers be sanctioned where they are not able to collect personal data from travellers who refuse to disclose?

34. We refer you to the answer to question two on the free movement of persons.

(f) Since UK border authorities collect passport data at the railway station of departure in France or Belgium before a traveller boards the train and the UK may refuse access on public security grounds, what are the reasons why Eurostar will also be required to collect API data?

35. As explained above, the e-Borders programme has a staged roll out. The effect of this is that the requirement to provide relevant data to the programme is being applied to particular carriers on particular routes. The programme has not been applied to Eurostar. We have been in continuing engagement with them as to how it might apply to them taking into account their business model, the information they hold and the information which the UK border authorities hold. It should also be noted that Eurostar (UK) Limited and Eurostar Group Limited are registered in the UK with the Information Commissioner's Office as data controllers in respect of the processing of personal data about its customers under the UK Data Protection Act 1998 and that some of the data is in the UK anyway. However, we will consider the unique position of the UK border authorities being at some points of departure for Eurostar in France and Belgium, albeit not at Lille in France, as we recognise that this has a significant impact in assessing the necessity of the processing. Before this mode/route is rolled out, we will need to devise a solution which ensures consistency across all borders and does not leave a gap in our border security. As we continue to finalise how e-Borders will be applied here, again we welcome the close engagement of the Commission.