-----Original Message-----
From: [Redacted name - UKBA]
Sent: 20 November 2009 5:43 PM
To: [Redacted contact details – European Commission]
Cc: Sedgwick Jonathan; [Redacted contact details]
Subject: Note on UK e-Borders system
Importance: High

Dear Aurel,

Please see attached which I hope will be helpful for you meeting with your legal services on Monday. I look forward to our call on Tuesday.

[Redacted contact details]
[Redacted contact details]
Tel: [Redacted contact details] Mob: [Redacted contact details] Email: [Redacted contact details]

[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

20 November 2009

Aurel CIOBANU-DORDEA

[Redacted contact details]
[Redacted contact details]

Dear Aurel

Thank you for your call yesterday – as ever, I was very grateful for your time.

As I understood our conversation, a final decision from the Commission on Pilot Complaint 348/09/JLSE ('the Complaint') is imminent and that pivotal to this will be the legal view (from the Commission Legal Services) on the 'legal base' point – the legal basis for a carrier transferring passenger data collected and held in another Member State from that State to the UK. You mentioned that you would be meeting your legal advisors on Monday, that they would provide their view and you have agreed to then let me know the outcome of that (we agreed I would call you at 15:00 GMT on Tuesday). We agreed that it would be helpful, in that context, if I were to pull together what remains outstanding from the UK side and send this to you in advance of that meeting. Please, therefore, find attached:

Annex A: a further paper setting out, in detail, our legal argument on the legal base point. This expands on both the email I sent to you and your team on 9 October and on the presentation given by the UK delegation at last weeks Art 29 sub group;
Annex B: Our response to the questions raised by you and your team when we met with you in Brussels on 6 October;
Annex C: Our response to your latest points on how we ensure that the commitments we have provided will be effectively applied in practice by our officials, specifically officers at the border.

All of these further sets of advice are in response to direct requests from you or your team and therefore address specific points. It is vitally important, therefore, (especially given the length of time this issue has been ongoing), that they are read in the broader context of our position, which is formed not only from that which I attach here but also what we have already sent to the commission previously. Specifically:

21 May – Our original response to the Complaint made to the Commission
24 August – Jonathan Sedgwick letter to Jonathan Faull
24 August – Our response to supplementary questions on Free Movement of EU citizens and their family members and to Data Protection aspects attached as an annex to the letter to letter to Jonathan Faull
9 October – my email to you setting out the summary of our legal position on the legal base point.

As I mentioned during our call, our feeling was that the Article 29 sub group went well and the feedback we received was that our attendance was enormously helpful. It was also made clear to me that on the outstanding issue, the legal base point, the Data Protection authorities [are very unlikely to reach consensus and] will look to the Commission to provide the lead in a matter they consider to be within the Commission's competence to determine given it concerns the interpretation of the Data Protection Directive. The key point for us is that they have been quite clear that they will accept the lead the Commission provides. We now hope we have provided everything the commission needs to make this decision and take this lead. And of course we believe that we have made a compelling cases, legally as well as politically, that our e-Borders system is fully compatible with European law, and that on what appears to be the key outstanding issue – the legal base point – we have clearly set out a convincing rationale that a legal framework clearly exists within the terms of the Data Protection Directive.

You asked – given that the key outstanding issue is the legal base point – that this response is addressed directly to you and your team within the Commission, as they (in conjunction with your legal team) are likely to be the final arbiters of the complaint. I hope you do not mind, however, that I am also copying this note to the offices of Jonathan Sedgwick on this side and of Jonathan Faull on the Commission side. They have maintained a helpful dialogue throughout this process and it is important they are both kept informed. I should also let you know that the UK Home Secretary is likely to write personally to the Commissioner, Jacques Barrot, in the next few days specifically about this and to underline the importance to the UK of a prompt and appropriate resolution of the Complaint.

We clearly feel we have now provided enough argument, evidence and reassurance to show that the UK's e-Border's system is fully compatible with European law. We now invite you to reach that same conclusion

Yours,

[Redacted name - UKBA]

Annex A

Introduction

1. As you know, a UK Border Agency delegation appeared before the Article 29 Data Protection Directive sub-traveller working group on 12 November to answer their questions on the UK's e-Borders programme. This Group included representatives from different parts of the Commission. The delegation began by making a presentation to the Group on what it had understood to be the central issue for resolution by the Commission of Pilot Complaint 348/09/JLSE ('the Complaint') – being the legal basis for the transmission to the UK of passenger data collected and held by a passenger carrier established in another Member State ('the legal base argument'). The UK notes that the Group did not ask any questions about the 'legal base argument' or challenge our position (on that the legal base argument) as set out in any way. Therefore, the UK assumes that the Commission is now able to accept that data can be transmitted from a carrier solely established in another Member State to the UK in accordance with Article 7(f) of the Data Protection Directive 95/46/EC (the 'Data Protection Directive')[1]. The UK has prepared this paper setting out its legal base argument in detail to assist the Commission. This expands on the e-mail sent by [redacted name] to Aurel Ciobanu-Dordea dated 9 October 2009 (3:33pm, UK time) and should be read with its detailed first and supplementary written responses to the Complaint.

Background

2. As you are aware, all passenger carriers operating services into and out the of the UK can be requested to provide information about their passengers, crew and service in advance of the arrival in or departure from the UK. This legal obligation is clearly established in UK national legislation. Some carriers have raised the question of whether the requirement to provide this passenger data is compatible with European Community law on the free movement of persons and on data protection. The Commission indicated at the meeting on 6 October that it is likely to conclude that the e-Borders programme is compatible with the law on free movement of persons. This note provides further clarification as to the data protection ground of Complaint.

[1] OJ L 281, 23.11.1995, p.31.

3. This paper sets out the extent to which the Data Protection Directive can be said to apply to the e-Borders programme. As set out below, the UK considers the majority of the passenger data that may be required is outside the scope of the Directive given the purposes for which it is requested. To the extent that it can be said some data remains within the scope of the Directive, then the majority of that remaining proportion will already be processed and controlled within the UK and be subject to the UK's data protection legislation transposing the Directive. This means that legal base argument does not arise. It is only arguable the legal base argument arises regarding a small minority of the remaining passenger data – to which the UK considers is strong view, that data can be transferred from another Member State to the UK compatibility with the Directive, under Article 7 is set out in detail in this paper.

Scope of application of the Data Protection Directive: Articles 3(2) and 13

4. As a preliminary point, it is important to recall the legislative basis and purposes for which the data is requested and can be used. The data can only be requested by the police for police purposes; by Her Majesty's Revenue and Customs (HMRC) for customs purposes and by the UK Border Agency for customs or immigration purposes. These purposes are defined and limited in national legislation. These agencies can only exchange the data they have collected under specified powers with each other if it is likely to be of use, respectively, for police, customs or immigration purposes. The main reason for collecting the data then is to use it for national security, public security, law enforcement including the prevention, investigation, detection and prosecution of criminal offences arising from breaches of immigration law (such as human trafficking) as well as border control.

5. The Commission will be aware that Article 3(2) Data Protection Directive provides that it shall not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law and in any case to processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law.. Given the specified purposes for which the data can be collected and used by the UK agencies, there is a compelling argument that the Directive is not applicable to the e-Borders programme. Further, to the extent that the e-Borders programme is within the scope of the Directive, Article 13(2) provides that Member States may adopt legislative measures to restrict the scope of the rights and obligations arising under that Directive where the measures concerned are necessary to safeguard national security, public security and law enforcement. Again, on this basis the application of the Directive would be limited.

A passenger carrier established in the UK and who processes passenger data in the UK

6. In respect of data protection, most passenger carriers already collect the information contained in the travel documents of passengers in the course of their business for accounting, auditing and business records purposes. The carriers can only collect and process this data in accordance with the

provisions of the Data Protection Directive as they are implemented by the domestic laws of the Member States.

7. The Data Protection Directive obliges a data controller who is established on the territory of several Member States to abide by the requirements of the law in each of them[2]. By the very nature of their business, carriers are required to operate from a number of different establishments in different countries. For instance, in order to assign seating and baggage tags, order food requirements, compile passenger lists and charge for overweight baggage, an airline who has a headquarters outside the UK must nonetheless maintain an establishment within the UK so that it can run its business in and out of the UK. The establishment in the UK, for a variety of reasons, such as for the tracking of missing baggage or the sale of last minute tickets for travel, will process personal data within the UK relating to incoming and outgoing services

.

8. The UK notes that as far as it is aware all of the carriers that e-Borders would apply to are likely to have some form of establishment within the UK and to be processing at least some, if not all of their passenger data in the UK. For example, 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[3]. These include Air France, Alitalia, Iberia, Brittany Ferries operating as BAI (UK) Limited, Eurostar (UK) Limited and Eurostar Group Limited

.

9. Accordingly, the majority of passenger data which a passenger carrier operating services into and out of the UK would be required to send to the e-Borders programme, would already be processed within the UK by an establishment of the carrier as a part of their standard business practice. That establishment is a data controller established in the UK and is subject to UK data protection legislation. Those carriers will be subject to a legal obligation, in terms of Article 7(c) of the Data Protection Directive, under UK law to provide the passenger data to the relevant UK border agencies when requested to do so.

10. The Commission confirmed at the 6 October meeting that passenger data held in the UK in respect of flights leaving the UK would be subject to UK Data Protection legislation. This would enable the UK authorities to request the passenger data from any passenger carriers operating a service departing the UK.

.

11. Our firm view is therefore, that the 'legal base argument' is only relevant in respect of the minority of passenger data which can genuinely be said to be collected, stored and processed only in another Member State by a passenger

---

[2] See Article 4(1)(a) and recital (19) of the Data Protection Directive.

[3] 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

carrier who is solely established as a data controller in that State and not in the UK.

12. It is assumed that the passenger data sought is already lawfully collected in that other Member State. The Community legislature has already accepted the principle that passenger data collected by carriers for their purposes can be used for the purposes of border security and law enforcement provided it is consistent with the Data Protection Directive[4]. Further, recital (8) of the Advanced Passenger Information Directive specifically records the freedom of Member States to retain or introduce additional obligations for aircarriers or other transport carriers. Accordingly, the provision of passenger data from the carrier to the UK authorities for these same purposes should not constitute processing which is incompatible with the purposes for which it was obtained by the carriers[5].

A passenger carrier established solely in another Member State and who processes passenger data in that State: legal basis for the transfer of the data to UK authorities - Article 7 Data Protection Directive

(i) General comments on Article 7: no territorial restriction on application

13. As set out in the UK's formal replies[6] and raised again at the meeting on 6 October, the UK considers that these passenger carriers can legitimately process the passenger data, in transferring it to the UK authorities, because one or more of the criteria set out in Article 7 of the Data Protection Directive applies. The Commission suggested on the 6 October that the criteria in Article 7 may have a territorial restriction – ie that the all of the purposes or circumstances identified which may make the processing of personal data legitimate under the Directive could only arise within the State of which the data controller is established. We respectfully disagree and suggest that the provision should be interpreted in another manner for the reasons set out below.

.

14. There is no explicit territorial restriction within the terms of Article 7. If this had been the intention, then the Directive would have been explicitly worded to restrict the application of this article to within the domestic sphere of a Member State. One of the purposes of the Directive is that Member States shall neither restrict nor prohibit the free flow of personal data between those States for reasons connected with protecting personal data (see Article 1(2) and recitals (7) to (9)). This interpretation is also supported by the closing wording of Article 28(6) which specifically provides for the scenario whereby

[4] See recital (12) of Directive 2004/82/EC on the obligation of carriers to communicate data ('the Advanced Passenger Information Directive'); OJ L 261, 6.8.2004, p.24.

[5] See Article 6(1)(b) of the Data Protection Directive; this argument was set out in detail in the UK's first written response to the Commission, see paragraphs 19-24.

[6] See the UK's supplementary written response to the complaint (August 2009), paragraphs 4-22.

the Supervisory Authority of one Member State can request his peer in another Member State to investigate particular processing. Logically this power can only have been intended to cover scenarios where there is some element of cross border activity, as any processing that was wholly domestic would only be of interest to one of, not both of the Supervisory Authorities. Because the Directive imposes common obligations on all Member States there is a common level of protection allowing the free flow of data. Thus in scenarios such as this where one state may require transfer of data from another for processing the correct procedure is for the Supervisory Authority of the second state to refer the matter to the Supervisory Authority of the first, as they are both regulating a common standard.

15. The Directive also specifically provides for the transfer of personal data from a Member State to third countries outside of the EU (in Chapter IV) where, generally, that third State maintains the same data protection principles and safeguards as those established within the EU. It seems conceptually inconsistent that, where those principles and safeguards legally apply within the EU, that same data cannot be transferred between Member States

.

16. It is clear that the provisions of Article 7 cannot have a territorial restriction. For example, Article 7(a), which refers to the data subject providing their consent to data processing, must mean that the subject could give their consent to the transfer of data outside of the Member State in which the data controller is established. The same should apply where this is necessary for the performance of a contract to which the data subject is party under Article 7(b)[7].

17. It is only where the passenger's consent to the transfer of their data to UK authorities has not been asked for, that the UK considers that Articles 7(c), (e) and/or (f) provide the basis on which the data can legitimately be transferred.

(ii) Article 7(c)

In respect of Article 7(c), carriers who operate passenger services into and out of the UK are subject to a legal obligation under national law to provide the passenger data when requested to do so by the UK authorities. In addition, for airlines, there is a legal obligation – in respect of some of the same passenger data – which arises from Article 29(c) of the Convention on International Civil Aviation 1944 as amended ('the Chicago Convention') to which all EU Member States are Contracting States[8]. For instance, airlines are required to ensure that each aircraft carries a list of names and places of embarkation and destination for each passenger – otherwise known as the passenger manifest. It is also relevant to consider recommended practice 3.47 of

[7] See British Airway's condition of carriage, at section 13, which can be found at: http://www.britishairways.com/travel/genconcarr1/public/en_gb; and also their privacy policy and statement on the provision of advanced passenger information at: http://www.britishairways.com/travel/fullpp/public/en_gb

[8] 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

Annex 9 to the Convention (entitled Facilitation) – which provides that Contracting States should introduce a system of advance passenger information. Accordingly, the airline passenger carrier is already, irrespective of the UK's e-Borders programme requirements, subject to a legal obligation within the State in which it is established to hold some of this passenger data and transfer it with the aircraft to the UK. Similarly, the maritime passenger carrier operating on intra-EU routes is under a legal obligation under EC law to maintain a certain amount of data about the carriers on board its ship[9]. These are separate legal requirements which pre-date the UK's e-Borders programme. The UK is not aware of any prior challenge by the Commission to these obligations.

(iii) Article 7(e) and (f): the UK authorities are the 'third party' to whom data is disclosed

Both Article 7(e) and (f) are based on the interests or role conferred on the third party to whom the data are to be disclosed – in contrast to the interests or role of the data controller. Article 2 defines a 'third party' to include a public authority and there is no requirement that only legal persons established in the same Member State as the Data Controller can qualify for this status as is to be expected in a Directive aimed at removing the obstacles to the flow of data and ensuring an equivalent level of protection across the community. In respect of e-Borders, the UK authorities are the third party to whom the passenger data would be transferred by the carrier established as a data controller in another Member State.

In Article 7(e), the processing must be necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the third party to whom the data are to be disclosed. We consider that the UK authorities are exercising official authority when requesting data under the e-Borders programme and also that there is a public interest in making such requests. Again, if the intention was that this should have a territorial restriction applied, then it would have been straightforward to make such explicit provision by replacing, for instance, 'public interest' with 'national interest' or 'official authority' with 'national authority'. In Article 7(f), processing can be necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed. Again, if the intention was that this should have a territorial restriction applied, such addition could have been included with an explicit reference to the State in which the controller or third party is established. There is no such restriction.

(iv) Articles 7(e) and (f): a public and legitimate interest for the UK and the EU

We consider that public and legitimate interests are wide terms that are not limited to a single domestic interest within a Member State but can also include the public or legitimate interest pursued in or by another Member State, a multi-Member State interest or a European wide interest. We consider the public interest in requesting this data is the same as that articulated in the Advanced Passenger Information Directive – being for the purposes of national security, the protection of public safety including

[9] See Article 5 of Council Directive 98/41/EC of 18 June 1998 on the registration of persons sailing on board passenger ships operating to or from ports of the Member States of the Community; OJ L 188, 2.7.1998, p.5

the prevention, detection and prosecution of crime as well as improving border control. The Community legislature, by passing this Directive, and by the Union adopting Agreements with the United States, Canada and Australia to oblige carriers to provide passenger name record to those States, has already accepted that the provision of this information is, in principle, proportionate and in the public and legitimate interest of the Community and the Union. This is underlined by the Commission proposal for a Framework Decision on Passenger Name Records which is currently under negotiations, including its application to intra-EU routes as well as, according to our understanding, the Commission's own plans for an electronic entry-exit system for the EU (or at least the main Schengen zone). Accordingly, there should be no dispute that there is a public and legitimate interest in the principle of collecting and using this passenger data from carriers for these specific purposes and that the Community legislature has accepted this.

There is a public and legitimate interest pursued by the UK, as the third party to whom the data would be disclosed, in collecting and using the passenger data in maintaining its national security, public security, law enforcement and border control. The UK has a right, under Protocol number three annexed to the Treaty on European Union ('the Frontiers Protocol')[10], to exercise at its frontiers with other Member States such controls on persons seeking to enter the UK as it may consider necessary for the purpose of verifying the right to enter the UK of EU nationals and their family members and of determining whether or not to grant other persons permission to enter the UK. The collection of relevant passenger data which would be presented at the border but in advance of travel to or from the UK reflects the right to exercise such frontier controls.

There is also a public and legitimate interest for the EU in the UK collecting the data and using it for the specified purposes. As set out above, the Community legislature recognised in the Advanced Passenger Information Directive that Member States could go further than the minimum provisions set out in that Directive. Increasingly, crime acts across borders, including within the EU. The UK uses the information collected by e-Borders to give effect to its obligations to enforce European Arrest Warrants under Council Framework Decision of 13 June 2002 on the European Arrest Warrant and the surrender procedures between Member States[11]. In the first ten months of this year 80 of 137 arrests at the border were of passengers travelling outbound from the UK to other EU member states. The offences for which those passengers were wanted include kidnapping/abduction (1), violence against the person (7), recall to prison (1), fraud (2), blackmail (1), and burglary(7). This indicates that the UK has successfully stopped a significant number of its own and other nationals from exporting crime to the EU. Further, since the UK is outside the external Schengen border, the collection and analysis of data from passenger carriers operating services leaving the UK taking passengers to other EU Member States provides better security for the Schengen States. The UK notes that the only two States which are operating a similar electronic border system on intra-EU routes – Spain and the UK – are the two states to have suffered most recently from significant terrorist attack.

---

[10] Protocol on the Application of Certain Aspects of Article 14 of the Treaty Establishing the European Community to the United Kingdom and Ireland; see Article 1.

[11] OJ L 190, 18.7.2002, p.1.

In addition, there are a number of other legitimate interests for the carrier, as data controller established in that other Member State, one or more of which may provide a proper basis for the processing of the data in accordance with Article 7(f). It is in the legitimate commercial interest of the carrier to wish to transfer the relevant passenger data in its possession to the UK when requested to do so because it will enable them to comply with a legal obligation. For instance, an air carrier will be under an obligation in the State in which it is established to maintain a passenger manifest for each service under the Chicago Convention (as set out above). A sea carrier is under an obligation under European Community law to record the name, gender and date of birth of every passenger on board its service[12]. There is also the commercial interest for the carrier established in its home State to comply with a statutory obligation which will apply to it when it operates its services in the UK. It is in the legitimate commercial interest of the carrier to wish to transfer the data to ensure the safety of its passengers in the knowledge that the UK authorities are analysing the data to determine whether any passenger poses a threat to public safety or security and that any intervention in respect of that passenger can take place swiftly on arrival in or departure from the UK. This maintains its public reputation as a safe and trusted carrier. A number of carriers in a number of Member States have previously decided it was in their interests to provide the data to UK authorities during the pilot Project Semaphore which ran from 2005 to 2008 which preceded the e-Borders programme.

In respect of Article 7(f), we acknowledge that any carrier would have to undertake the balancing exercise envisaged between the relevant legitimate interests – whether its own as the data controller or those of the third party (the UK authorities) – against the fundamental rights and freedoms of the data subject protected under Article 1(1) of the Directive. It is relevant to note that the EU has already determined that the transfer of relevant passenger data to Canada, for instance, strikes this balance in favour of the transmission of data. In this context, the UK is also mindful of the assurances it provided in the 6 October meeting about the work which the UK Border Agency is undertaking to provide further information to passengers about the programme and how they may exercise their rights under the Directive in respect of data which the UK authorities may hold about them.

In conclusion, following the 6 October meeting we respectfully invite the Commission to reject the Complaint by providing its opinion that a request for relevant passenger, crew and service information from passenger carriers by UK authorities under its e-Borders programme:

(a) is compatible with Directive 2004/38/EC on the right of citizens of the Union and their family members to move and reside freely within the territory of Member States;

(b) is capable of being compatible with Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data:

---

[12] See Article 5 of Council Directive 98/41/EC of 18 June 1998 on the registration of persons sailing on board passenger ships operating to or from ports of the Member States of the Community; OJ L 188, 2.7.1998, p.5.

(i) to the extent the e-Borders programme collects data for the purposes of national security and law enforcement purposes it is either excluded from the scope of the Directive by Article 3 or it constitutes a necessary measure to safeguard national security, public security and law enforcement under Article 13 of the Directive which restricts the application of the obligations and rights arising under the Directive;

(ii) since the transfer of personal data from a passenger carrier to the UK authorities for the further processing by them for the purposes of,national security, law enforcement as well as border control is not incompatible with the original purposes for which the data was collected;

(iii) where passenger data is processed in the UK by a carrier who operates a branch, office or agency through which the carrier carries on any activity in the UK, the provision of data to the UK authorities will automatically fall within the jurisdiction of the UK data protection legislation transposing the Directive since where a carrier is established in several Member States it must ensure that each of its establishments complies with the national law applicable as required under Art 4(1)(a) of that Directive;

(iv) where a passenger has consented to the transfer of his or her data to the UK authorities in accordance with Article 7(a) or the passenger is party to a contract with the carriers which requires the transfer of that data to UK authorities in accordance with Article 7(b);

(v) given passenger carriers operating services into and out of the UK are subject to a legal obligation under national law to provide relevant passenger data to UK authorities for the purposes of Article 7(c);

(vi) since the UK e-Borders programme collects passenger data for the purposes of national security, law enforcement as well as border control, it pursues both a common public interest and a legitimate interest for the purposes of Article 7(e) and (f) respectively and the UK authorities are a third party pursuing those interests on its own behalf and on behalf of the EU to whom the data can be disclosed in accordance with this provision;

(vii) because Articles 7(e) and (f) can constitute criteria for the legitimate processing of data by a carrier established in another Member State in transferring passenger data to the UK authorities.

Annex B

[NB **Annex B as at attachment to 6 November 8.49AM email below - note to Marie-Helene Boulanger, page 52]**

Annex C

1. You have sought legal guarantees that no EU carrier operating on intra-EU routes or EU national passenger or their family member will be fined and that no passenger will be denied boarding due to a refusal to provide advance passenger information to UK authorities under the e-Borders programme. The

UK set out its position in its original written response to the Complaint and re-iterated in its supplementary written response - as set out in the answers to questions 1 to 3 at Annex A of our 24 August letter to Jonathan Faull. The UK would not impose or apply a power where in its view there would be a breach of European Community law.

2. In respect of passengers, the first UK response, repeated in the supplementary response, stated:

> "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."

3. The rights of admission for EU nationals and their family members are clearly set out in this national legislation. UK Border Force officers must abide by this legislation. This sets out the limits of their powers to review EU nationals and their family members on arrival. There is no power for the Officer to refuse entry to or restrict departure from the UK because the passenger has not provided information in advance of travel to the carrier under the e-Borders programme. Copies of this legislation are set out in the guidance available to Officers operating at the UK Border.

4. Equally, the UK Border Agency would require a power in legislation to order a passenger carrier to deny boarding to an EU national passenger or their family member in advance of travel. There is no power in national legislation to do so. This in addition to the point above about the UK's obligations under European Community law to give effect to Directive 2004/38/EC.

5. In respect of a passenger carrier, as the UK has previously explained, there is a criminal offence in national law of failing to provide relevant passenger or service information when requested. However, it is significant that there is a statutory defence for the carrier of having a reasonable excuse for not providing the 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 in respect of a request made by a police officer). The final decision on whether to prosecute for this offence is for the independent prosecuting authority, the Crown Prosecution Service. In order to prosecute they must consider whether prosecution is in the public interest and whether there realistic prospects of success. In reaching a decision they would take into account the availability

of the statutory defence for the carrier and the fact that information could not be provided if the provision of that information would breach European Community law. .

6. We have already said in answer to question 2 of the supplementary questions, that 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. We are working with carriers to establish a process which makes clear when failure to provide data in respect of an individual EU passenger is down to the individual's refusal to provide this data rather than non-compliance on the part of the carrier. We would be pleased to share with you this guidance when the process has been finalised.