

Letters requested

Julie Gillis
e-Borders Programme Director
[Redacted contact details]
[Redacted contact details]
[Redacted contact details]
[Redacted contact details]

Tel [Redacted contact details]
Fax [Redacted contact details]
Email [Redacted contact details]
Web www.ukba.homeoffice.gov.uk

Jacques Barrot

12th June 2009

Dear Mr Barrot

I understand that you will be addressing the Data Protection Directive Article 29 Committee working group on 16/17 June, where a discussion on the UK's e-Borders system is due to take place. I thought therefore that you might find it helpful to have the current position from the e-Borders Programme.

You will be aware that a number of DPAs have raised concerns about e-Borders, especially in the context of recent correspondence between our departments. In advance of next week's meeting we thought it would be helpful to set out the UK position and we are therefore writing to all the DPAs in response to concerns they have raised. A copy of the letter is at Annex A.

Further to this, we have had meetings with some DPAs and expect that this additional information will allay their concerns. You will see that in the letter we have invited the DPAs to visit our Joint Border Operations Centre as you did earlier in the year and we hope that we will have the opportunity to demonstrate the benefits of e-Borders.

You will of course understand that e-Borders is a critical element of the UK's strategy for managing its borders. A strong UK border means a strong EU border. This must of course be balanced with proper safeguards. A balance we believe we have achieved with e-Borders and would be willing to attend the Article 29 Working Group to explain this position.

I hope you find this update useful, and I am of course available to answer any questions you may have on the issue.

Yours sincerely,



Julie Gillis
e-Borders Programme Director

[NB Annex A to Barrot letter (to EU DPAs) follows]

Julie Gillis
e-Borders Programme Director
[Redacted contact details]
[Redacted contact details]
[Redacted contact details]
[Redacted contact details]

Tel [Redacted contact details]
Fax [Redacted contact details]
Email [Redacted contact details]
Web www.ukba.homeoffice.gov.uk

12th June 2009

Ref: e-Borders Programme & data collection

I am writing to you about the UK Government's e-Borders Programme and our plans to collect passenger data from carriers on routes between EU Member States and the UK. We understand that e-Borders is on the agenda of the next meeting of the Article 29 Data Protection Directive working group. The aim of this letter is to ensure you have accurate information about e-Borders to inform your discussions.

e-Borders is a key component of the UK Government's strategy to strengthen and modernise border controls. We believe that the programme is an entirely appropriate response to the real risks we face, enabling us to target those who represent the most serious harm and speed up travel for the law abiding majority. It is designed to provide more information to the UK authorities of passengers in advance of travel to better inform decisions taken by officers on arrival in, or prior to departure from, the UK. The programme has been developed over a number of years in consultation with the European Commission, our national data protection authority and carriers. It is now at an advanced stage with over 55 carriers already collecting and sending data to the relevant UK authority, the UK Border Agency, and additional carriers and routes planned to come on-stream every week.

We would like to provide the following reassurances:

EU nationals and their family members have the right of entry to the UK in accordance 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 – the e-Borders programme imposes no additional requirement for entry.

We do not prevent last minute travel. There is no question of passengers being prevented from travelling due to not supplying information sufficiently far in advance of travel, nor is there a question of passengers having to complete any sort of questionnaire at check in.

We work closely with carriers to ensure that passenger flows are not affected by e-Borders, and there is no question of services being unable to operate due to the non-supply of data.

e-Borders is not an authority to carry scheme and does not issue instructions to carriers to prevent a particular service from travelling, or instructions to the carrier to prevent individuals from travelling.

Any future plans to develop an ATC scheme would be developed in consultation with the European Commission and would be in accordance with European law.

We consulted the UK national data protection authority, the Information Commissioner's Office, throughout the preparation of the national legislation bringing the e-Borders programme into force and, took their advice into account where possible. We continue to consult our Information Commissioner over the operation of e-Borders and their possible involvement in supervisions arrangements, particularly for the new National Border Targeting Centre. We are also consulting the Information Commissioner on the review of the Code of Practice governing the processing of data by the UK Border Agency, Police and Customs. Our view is that the programme operates in accordance with our national Data Protection Act 1998 which transposes the 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.

We use the Advance Passenger Information to identify individuals who have already come to the attention of the border agencies, including those identified by other Member States (in European Arrest Warrants for instance) and EU organisations such as Europol. We pass this information to front line officers so they can make a more informed judgement on those most likely to be of interest. This ensures greater border security for the UK and EU. It also means the vast majority of law abiding passengers have a faster border crossing.

Carriers transporting passengers on high risk routes can be required to provide reservation data (known as Passenger Name Record information) to the e-Borders system, but only if it is already being collected by the carrier in the normal course of their business. Using this, we establish patterns of passenger behaviour that our intelligence gathering has identified as being indicative of higher risk. We then use our computer systems to screen the Passenger Name Record data to identify any individuals who follow those patterns. Where this rules based targeting identifies a potential person of interest we will scrutinise the data further to identify additional factors that will increase or decrease the level of interest. Where the individual remains a high level of interest, this information will be passed to front line officers to consider. Again, this allows faster border crossing for the law abiding majority.

We also operate rules based targeting to identify, with the aim of protecting, those persons who may be at risk themselves, including vulnerable women and minors being trafficked for the purpose of exploitation.

We do not operate rules based targeting on the basis of ethnicity or religion.

Data is held in a secure database in a secure location, and accessed only by security cleared officers. All access is monitored and audited in line with the statutory code of practice.

We currently plan to keep data for 5 years in an active database and 5 years in an archive accessed on a case-by-case basis. This is consistent with the time period initially proposed by the Commission when it published its proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes. There are on-going discussions of data retention periods in the negotiations of this Framework Decision, and the UK will act in accordance with the outcome of those negotiations.

We have recently written to the European Commission explaining the legal basis for e-Borders, with specific reference to Directives 95/46/EC (the Data Protection Directive) and 2004/38/EC (the Citizens' Directive). A summary of the legal basis can be found in Annex A.

On this basis, UK legislation continues to apply and carriers are therefore required to provide data as and when requested by e-Borders and failure to do so would risk their liability to sanctions. This is not a preferred route for the UK Government but we may need to resort to such measures if the implementation of our e-Borders programme is compromised.

The implementation of e-Borders is at an advanced stage and resolving any concerns is a high priority for us. I hope that this letter will inform a full discussion of all aspects of e-Borders at the meeting next week and results in a clear position going forward.

We would like to invite you to visit our Joint Border Operations Centre and to allow us to demonstrate how e-Borders operates in practice. I would also like to assure you that we take data protection seriously and are keen to work with you to address any concerns you may have.

I look forward to hearing from you.

Yours sincerely,

A handwritten signature in dark ink, appearing to read 'Julie Gillis', written in a cursive style.

Julie Gillis

Annex A: Legal Basis [NB this is Annex A to 12 June letter to EU DPAs]

UK legislation requires commercial carriers and operators of all air, rail and maritime vessels scheduled to arrive in or depart the UK, to submit detailed information prior to travel, when requested to do so. The legal basis to require this data is established in the following UK legislation:

- Paragraphs 27 and 27B of Schedule 2 to the Immigration Act 1971 and subsequently in secondary legislation made under these provisions (Statutory Instrument 2008/5);

- Section 32 of the Immigration, Asylum and Nationality Act 2006 and secondary legislation made under this provision (Statutory Instrument 2008/5); and
- a Direction issued by the Commissioners for Her Majesty's Customs and Revenue under section 35(1) of the Customs and Excise Management Act 1979.

Further information on the legislative framework can be found on the UK Border Agency website¹. This legislation transposes Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data. You will be aware that the Directive does not prohibit collection of data beyond the requirements set out in the articles, and it is on this basis that we have legislated domestically to require carriers to supply data on journeys between other Member States and the UK.

e-Borders operates under strict data protection controls. The UK transposed the EC Data Protection Directive (Directive 95/46/EC) through its Data Protection Act 1998. When it transposed the Directive, the UK, like most other Member States, applied the principles set out in the Directive to the processing of personal data for the purposes of both the European Community Treaty ('the first pillar') and Title VI of the European Union Treaty ('the third pillar'), including in the field of police and judicial co-operation in criminal matters.

A statutory Code of Practice² covering the processing of passenger data by the UK Border Agency, Police and Customs has been drawn up in consultation with the UK national Data Protection Authority, the Information Commissioner's Office, and sets out the ways in which the border agencies will comply with the safeguards set out in our Data Protection Act. Accordingly, in our view, the acquisition of data under e-Borders is compatible with the provisions of the Data Protection Directive.

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/EC, is set out in UK law in regulation 11 of the Immigration (European Economic Area) Regulations 2006 No. 1003. The UK's border authorities may check the documents presented on the arrival of EU citizens at the UK's border crossing points. The added value of e-Borders is that within 30 minutes of a departure carriers will supply a departure confirmation message of those travelling on the service to the UK's border authorities. There is no power in the legislation enabling the e-Borders' programme to prevent a flight from departing. The programme enables United Kingdom border checks to be more targeted in combating criminal activity and will facilitate more efficient processing for the vast majority of passengers.

EU passengers travelling 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. The travel document information of a passenger or crew member which may be requested from the carrier prior to arrival or

¹ <http://www.ind.homeoffice.gov.uk/aboutus/workingwithus/transportindustry/ebordersrequires/legalpowers/>

² <http://www.bia.homeoffice.gov.uk/sitecontent/documents/managingourborders/eborders/codeofpractice/>

departure is derived from the person's passport, identity card or other type of identification already relied upon by the passenger³ to travel.

-----Original Message-----

From: BALTAZAR Telmo (JLS)
Sent: mardi 30 juin 2009 13:20
To: [Redacted name - UKBA]
Cc: [Redacted contact details]
Subject: UK e-Borders – list of questions

Attachments: 2009 06 29 Questions to UK on free movement and dp-final version.doc;
Picture (Metafile)

Dear [Redacted name]

As agreed at the meeting on 23 June with the UKBA team I am sending you the list of questions from the Commission side regarding some elements of the UK e-Borders project. We would be grateful to receive your answers at the earliest possible opportunity and preferably before the end of August.

As agreed at the meeting we hope to be able to pursue the conversation and if needed we can convene a further meeting.

Thank you very much for your cooperation.

Best regards,

Telmo Baltazar

Telmo Baltazar

[Redacted contact details]

[Redacted contact details]

[Redacted contact details]

Office: [Redacted contact details]

³ See paragraphs 1(b) and 2(b) of Schedule 2 and paragraph 1(b) of Schedule 3 to the Immigration and Police (Passenger, Crew and Service Information) Order 2008 (No. 5) which can be found at: http://www.opsi.gov.uk/si/si2008/uksi_20080005_en_1.

T: [Redacted contact details]
Email: [Redacted contact details]

[NB ATTACHMENT TO 30 JUNE E-MAIL FOLLOWS]

UK E-BORDERS

REMAINING 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

If the requested data are checked against existing "watchlists" before boarding, the UK authorities cannot deprive EU citizens and their family members of their rights under Chapter VI of Directive 2004/38/EC, as described in our letter of 19 March 2009.

Could the UK authorities confirm that carriers would not be asked to deny boarding to EU citizens or their family members on any grounds?

2/ Sanctions

The UK scheme provides for sanctions for carriers failing to provide requested data (*Section 27 of the Immigration Act 1971 and Section 34 of the Immigration, Asylum and Nationality Act 2006*). These sanctions could instigate commercial carriers to adopt internal policies to deny boarding to EU citizens who do not provide them with the requested data. This could represent an obstacle to free movement of EU citizens.

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)?

3/ Availability and collection of data

It would be against the Free Movement Directive (2004/38) to have a situation in which EU citizens and their family members are turned back at the UK border or face difficulties entering the territory of the UK because their data are not available to the border guard (for whatever reason). The administrative formalities at the border cannot go beyond gathering/processing the information mentioned in the Directive.

The documents to be presented to obtain access into the territory of a Member States are exclusively those mentioned in the Directive. The early availability or last minute collection of data cannot be made a condition for EU citizens and their family members to exercise their right to free movement.

Could the UK authorities confirm this?

B) DATA PROTECTION

Without prejudice to the concerns and issues raised from the perspective of the free movement of persons, the current UK E-borders scheme also raises questions relating to the protection of personal data that need to be addressed in order to have a full and complete picture of the system.

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

Carriers to UK are required to collect and process personal data of travellers in the Member State of departure so that they may communicate them to UK border authorities. The collection of personal data in the Member State of departure constitutes processing of personal data activity that has to be carried out in accordance with the data protection legislation of the Member State of the carrier (cf. Article 4(1)(a) of Directive 95/46/EC, e.g; French law for Air France, or Italian law for Italian air carriers).

Pursuant to Directive 95/46/EC, for a processing activity to be lawful it must have an appropriate legal basis (cf. Article 7 of Directive 95/46/EC).

It is therefore necessary to determine 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. Since the API Directive does not apply for intra EU flights (cf. Article 2(b) of Directive 2004/82/EC), this Directive cannot constitute the Community legal basis for the collection and transfer of personal data of passengers of such flights to the UK.

As part of this exercise, it would also be necessary to determine if UK legislation requires the collection of data which is additional to that normally collected by carriers in any event – in other words, personal data that carriers would not collect but for the UK legislation.

2/ Data quality and proportionality principles

Directive 95/46/EC requires that the processing of personal data be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (Art. 6)(b).

It would be useful to know the kind and number of personal data that shall be processed, and whether citizens shall be required to communicate all the personal data laid down in UK legislation.

What would be the consequences for an individual who refuses to disclose his/her personal data to a carrier? Should carriers be required, directly or indirectly (e.g. by fines) to collect all the personal data laid down in UK legislation? 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? Will carriers be sanctioned where they are not able to collect personal data from travellers who refuse to disclose?

In the case of EUROSTAR journeys from France/Belgium to UK, UK border authorities already control and collect travellers' passports at the railway station of departure in France or Belgium, before a traveller is allowed to board the train. Since UK border authorities will always collect them before the train leaves and may refuse access to the train on public security reasons, it would be useful to know the reasons whereby Eurostar will be required to also collect API traveller data in addition to this data.

3/ **Sensitive data**

UK e-borders will entail the processing of sensitive personal data, within the meaning of article 8 of Directive 95/46/EC (See Code of Practice, section 4.4).

Why will sensitive data be processed, and under what conditions? Is such information required from each traveller including EU citizens? What specific safeguards are contemplated?

4/ **Retention periods**

The period of retention of personal data processed by UK e-borders would be 5 years followed by an additional 5 years period of archiving.

Is this retention period applied to all personal data processed in the system? Is there a distinction between *bona fide* travellers not being identified as dangerous or criminals and those who represent a threat to the public security, defence or are serious criminals? Will data be retained merely on the basis that it might possibly become relevant at some unknown time in the future?

5/ **Rights of citizens**

Are citizens informed in a clear manner of their rights (access, rectification, erasure or blocking)? How are they informed?

Is there a central service or body responsible for dealing with requests and complaints of citizens who avail themselves of their data protection rights? How may a citizen exercise his/her rights to access to his/personal data and to rectify, delete and block his/her personal data?