Response to a consultation from EFSA's DPO under Article 46(d) of Regulation (EC) No 45/2001 (case 2009-390)

1. Procedure

On 1st April 2009, in the context of the prior check of EFSA "Declaration of Interests (DoI) data processing operations" (case 2008-737), the EDPS received an email from the Data Protection Officer (DPO) of EFSA raising certain issues relating to the transfer of personal data of EFSA external experts by EFSA to American Express Corporate Travel SA (AMEX).

On 5 June 2009, the EDPS sent a letter to the DPO of EFSA to inform him that these issues would be analysed separately from the prior checking notification 2008-737. In this letter, the EDPS requested further information on the data transfers between EFSA and AMEX.

By letter dated 24 June 2009, the DPO provided the EDPS with further information, including the Data Protection Covenant signed between EFSA and AMEX and a model purchase order for "pre-paid ticket". The EDPS asked further clarifications to the DPO, which were received on 12 March 2010. On 30 November 2010, the EDPS sent the summary of the facts to the DPO, whose comments were received on 7 December 2010.

2. The Facts

2.1. EFSA relationship with AMEX

After EFSA's contract with a travel agency was terminated at the end of March 2009, EFSA entered into a service framework contract with AMEX. AMEX was chosen as a result of an inter-institutional international call for tenders for travelling services coordinated by the European Commission.

In order to ensure proper handling of personal data in the context of the framework contract entered into with AMEX SA (Brussels branch of AMEX), a Data Protection Covenant ("the Covenant") was signed between EFSA and AMEX (together with UVET SpA, a company incorporated in Italy). The EDPS understands that the text of the Covenant is based on a model provided by the European Commission.

Pursuant to the Covenant, EFSA appointed AMEX as a processor for a part of the processing, while AMEX is acting as a data controller for another part of the processing. Article 2 of the Covenant provides that "*With reference to Art. 2 of Directive 95/46/EC and Regulation No (EC) 45/2001 AMEX will be appointed as Controller in relation to the processing of the Profile Data and as Processor in relation to the processing of the Travel Data*". Article 7 of the Covenant further

establishes that the rights of travellers with respect to data processed by AMEX as controller (i.e. profile data) are governed by Directive 95/46 and EU/EEA national laws implementing the Directive; the rights of travellers with respect to travel data, for which AMEX only acts as a processor on behalf of EFSA, are subject to Regulation (EC) No 45/2001 as EFSA remains responsible for that part of the processing as data controller.

2.2. Options initially considered for transferring data to AMEX: Use of the DoI database for providing AMEX with external experts' identification data

At the start of their cooperation, as agreed in the Covenant, AMEX requested EFSA to provide identification data on all potential travellers on the ground that this information was necessary to ensure the provision of the travel services. To satisfy this request from AMEX, EFSA had to identify not only EFSA staff but also external experts involved in the activities of EFSA constituent bodies for whom EFSA bears the travelling costs. At the time AMEX started providing travel services to EFSA, ensuring the continuity of service was a major concern for EFSA given the fact that the organisation of missions is an essential and critical support task for EFSA towards its experts. EFSA came across the practical difficulty of finding a way to provide the identification data of those external experts for whom EFSA bears the travelling costs. In those circumstances, EFSA consulted the DPO on several options that EFSA was considering for transferring external experts' identification data to AMEX, which implied using the electronic system supporting the handling of annual Declarations of Interests (DoI).

At the time the cooperation started with AMEX, **EFSA was considering arranging a systematic transfer** of external experts' identification data available from the DoI database. EFSA then envisaged the **possibility to arrange for a single transfer** of an Excel sheet to AMEX containing identification data of external experts pulled out from the DoI database. However, after consulting with the DPO and considering that a consultation was pending at the EDPS on this issue, EFSA decided that all expert travellers provide their identification data themselves to AMEX by means of the pre-paid order form they have to fill in at the time a pre-paid ticket is requested.

While EFSA so far refrained from doing any transfer of data extracted from the DoI database, the DPO however indicated that it is possible that at one point in the future EFSA could provide AMEX **with a print out of the DoI electronic system** on the ground of the *"needs for service optimisation to confront ever becoming more difficult travelling conditions*".

2.3. Options chosen for transferring data to AMEX

After consulting with the DPO, EFSA decided that no basic travel information would be extracted from the DoI database, and that all travellers provide themselves -directly or indirectly- their identification, profile[1] and travel[2] data to AMEX. As EFSA stated,

[1] According to the Data Protection Covenant, "'Profile Data' concern the Basic Traveller's Data plus all additional personal data provided as necessary or freely agreed by the traveller to AMEX directly or indirectly via EFSA and subsequently sent to transport companies, hotels or car renting companies: name and surname on identity documents (if different from Basic Traveller's Data), identity cards or passport number, nationality, date and place of issue, end of validity date, possibly professional credit

the consideration of the rights of data subjects was a substantial element in opting for this current alternative.

Therefore, at the start of the contract with AMEX, EFSA staff submitted directly their profile data[3] in an online module of AMEX. The personal data of external experts involved in the activities of EFSA constituent bodies are case-by-case transferred to AMEX by means of the completed EFSA pre-paid order form.

Furthermore, EFSA informed the EDPS that mission specific travelling data of EFSA staff and external experts are provided to AMEX on a case-by-case basis along EFSA mission workflow through the pre-paid order form. The mission specific data collected in the pre-paid order form and transferred to AMEX include the following data: unit, mission number, meeting FSA number, budget line, meeting dates and schedules, meeting title and place, EFSA contact person, as well as traveller's mobile phone, email address and address, inbound (date + time) and outbound (date + time). The data are handed over by EFSA to AMEX.

2.4. Onward data transfers by AMEX

The EDPS notes that, without distinguishing between its role as controller or processor, Article 3.3 of the Covenant provides for the possibility for AMEX to transfer personal data collected about EFSA staff and external experts to a number of recipients, including:

(i) AMEX's suppliers and AMEX affiliated companies for purpose of making travel reservations,
(ii) EFSA for purpose of reporting and verifying deviation from the travel policy of the organisation,
(iii) third parties for purpose of making reservations, producing reports, collecting payments, and auditing AMEX services upon request from EFSA, and
(iv) databases of AMEX in EU/EEA or outside in third countries which have been deemed to offer an adequate level of protection or to recipients located in third countries with which AMEX entered into an agreement that contains appropriate contractual clauses, in particular the standard contractual clauses approved by the European Commission for international transfers. No purpose for these transfers is mentioned in the Covenant.

3. Legal analysis

The EDPS will first analyse the concerns raised by the DPO as to the use by EFSA of the Declarations of Interest database for purpose of providing external experts' identification data to AMEX.

---

card number, and other relevant information which the traveller may have agreed to provide directly or indirectly (e.g. frequent traveller scheme numbers and traveller preferences for sitting and meal) ".

[2] According to the Data Protection Covenant, "'Travel Data' cover Basic Traveller's Data plus all additional data concerning the travel itself provided by the traveller directly to AMEX or indirectly via EFSA, with the aim of using the services: planned departure and return times from or to the workplace, beginning and ending times of professional engagements on the place of mission, or generated by the use of the services: means of transportation used, hotel name(s), invoice(s)".

[3] The following profile data are compulsory: first name, surname and e-mail account.

The EDPS will also analyse additional issues which he came across in the course of the review of the case, concerning the necessity and the proportionality of the data transfers to AMEX, the double status of AMEX who acts as a controller and as a processor, and onward transfers by AMEX to recipients outside the EU/EEA.

3.1. Would the envisaged use of the DoI database be in accordance with the purpose limitation principle (Article 4(1)(b) of Regulation 45/2001)?

In view of the purpose limitation principle set forth in Article 4(1)(b) of Regulation (EC) No 45/2001 ("the Regulation"), data collected in the DoI database should only be processed for purpose of managing annual declarations of interests and verifying that a concerned individual has no conflict of interest, and should not be further processed in a way incompatible with these purposes.

The DPO argued that the extraction of external experts' identification data from the DoI database for purpose of communicating them to a travel agency might not be incompatible with the original purpose of the data collection since *"travel arrangements serve the purpose of involvement in EFSA activities and meetings for which experts have submitted their DoI"*.

As was described to the EDPS in the prior check case 2008-737, the processing of annual DoI aims at ensuring that the concerned individuals have no conflict of interests which could interfere with their activities carried out for EFSA. Several categories of persons working for EFSA are required to submit an annual DoI pursuant to Article 37 of Regulation 178/2002 (EFSA founding Regulation), "*indicating either the absence of any interests which might be considered prejudicial to their independence or any direct or indirect interests which might be considered prejudicial to their independence*". This requirement was extended to external experts by Decision of the Executive Director[4]. Failure from external experts to submit their annual DoI will lead to sanctions, including not being invited and/or not being allowed to attend a meeting.

While the submission of the DoI is a pre-requisite for external experts in order to be involved in the activities of EFSA and while the DoI database serves the purpose of verifying that experts can participate in the work of EFSA, the processing does not entail as such that some of these data would be transferred to an external private recipient for purpose of facilitating travel arrangements, even when such travelling arrangements would be linked with the activities undertaken by external experts for EFSA. These are two different purposes: on the one hand verifying that an expert has no conflict of interest so that he can be involved in the work of EFSA and on the other hand ensuring that an expert can make travelling arrangements through the travel agency AMEX.

Having considered this, the EDPS finds that any further processing by EFSA of data processed in the DoI database -in whatever format, be it extraction in Excel sheets, systematic transfer or print out of the database- for purpose of providing to an external

[4] Article 13(3) of Decision of the Executive Director Concerning the Selection of Members of the Scientific Committee, Scientific Panels and External Experts to assist EFSA with its Scientific Work.

recipient (AMEX) the identification data of persons who can benefit from AMEX travel services would not be considered compatible with the initial purpose of the data collection and processing since it would serve a totally different purpose. Therefore, such a further processing by EFSA would not comply with Article 4(1)(b) of the Regulation.

By way of an exception, Article 6 of the Regulation authorises a structural change of purpose only if strict conditions are met. This would notably require that the use of DoI data for purposes other than those for which they were collected is expressly permitted by the internal rules of EFSA for clearly justified grounds and that individuals concerned are provided with appropriate information[5] about the further processing of their data. This is not the case; therefore any further processing of DoI data by EFSA for a different purpose from the one for which they were collected would not be justified under Article 6 of the Regulation.

3.2. Are EFSA data transfers to AMEX in compliance with the Regulation?

Two specific types of data transfers raise particular data protection concerns: the transfers of all potential users' identification data and the transfers of travellers' mission specific data. They will be analysed separately below.

3.2.1. Transfers of all potential travellers' identification data

Article 6 of the Covenant required EFSA to transfer all Basic Traveller's Data[6] to AMEX at the beginning of the contract: "*Basic Traveller's data of all Commission's staff that may potentially use the services provided by AMEX will be transferred by the Client to AMEX at the beginning of the Contract and subsequently updated as needed for its performance subject to the provisions of Chapter 3 and 4 of this [Data protection] Covenant*".

The EDPS now understands that no such transfer occurred since, as explained by the DPO, EFSA staff provided their identification data themselves directly to AMEX and external experts' data were communicated to AMEX on a case-by-case basis when the use of its service was needed.

The EDPS however wants to underline that the requirement stated in Article 6 of the Covenant would, if implemented, lead to a breach of the Regulation. In particular, the processing of data in view of fulfilling this contractual requirement would not have any legal basis under Article 5 of the Regulation. Furthermore, the bulk transfer of identification data of all EFSA staff and external experts involved in the activities of EFSA constituent bodies would not seem necessary and justified under Article 8(b) of

[5] The EDPS underlines that he has not been provided with any data protection notice in relation to the DoI database, despite his recommendation in the prior checking opinion on the DoI database that EFSA should adopt a data protection notice compliant with Articles 11 and 12 of the Regulation (case 2008-737).

[6] "Basic Traveller's Data" cover identification and contact data of each member of EFSA's staff or third persons whose travelling is paid by EFSA who may use the services of AMEX. Basic Traveller's Data comprises: title, name, surname, office address, place of work, e-mail address and office telephone number. As concerns EFSA's staff, the Unit under which the traveller resorts is also indicated.

the Regulation. Finally, such a transfer would result in transferring an excessive amount of data, which would be in breach of the proportionality principle laid down in Article 4(1)(c) of the Regulation.

3.2.2. Transfers of travellers mission specific travelling data

The EDPS understands that EFSA provides AMEX with mission specific travelling data on a case-by-case basis along EFSA mission workflow. Mission specific travelling data include unit, mission number, meeting FSA number, budget line, meeting dates and schedules, meeting title and place, EFSA contact person, as well as traveller's mobile phone, email address and address, inbound and outbound (date + time).

Firstly, it can be questioned whether the transfer of all the mission specific data to AMEX is necessary for the purpose of rendering travel services, as required under Article 8(b) of the Regulation. While the EDPS understands the necessity of transferring the contact details of the traveller and of an EFSA contact person, e.g. for purpose of informing the traveller of a flight's cancellation, the EDPS has however not seen any evidence supporting why the transfer of all other data would be necessary.

Secondly, the transfer of mission specific data to AMEX also raises concerns in respect of the proportionality principle. Article 4(1)(c) of the Regulation requires that data are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The EDPS emphasizes that only data that are strictly necessary for the travelling arrangements should be passed on by EFSA to AMEX, which is not only a risk for the activities of EFSA but also for the activities of the EU.

Consequently, the EDPS considers that the transfer of all mission specific data of EFSA staff and external experts does not meet the conditions of Article 8(b) and Article 4(1)(c) of the Regulation.

3.3. Legal implications of AMEX acting as controller for a certain part of the processing and as processor for another part of the processing

As described in section 2.1 above, the Data Protection Covenant -which is based on a model provided by the European Commission- states that AMEX is a data controller in relation to the processing of the profile data and a processor in relation to the processing of the travel data.

The EDPS notes that it is not clear why AMEX acts in the capacity of controller for certain data and in the capacity of processor for other data. The role and responsibilities of AMEX as controller and as processor are not clear, nor are the differentiation of the types of data under which AMEX acts as controller and as processor. For example, the processing of "Basic Traveller's Data" falls into the two categories.

The EDPS emphasizes that the capacity under which AMEX acts cannot just be artificially defined in an agreement; such capacity must derive from concrete elements

which demonstrate that the requirements for being considered either as a data controller or as a data processor are effectively met.

The EDPS also has concerns about the use by AMEX, in its capacity of controller, of EFSA travellers' data for its own purposes. The EDPS recommends that further clarifications are obtained from AMEX on this issue.

Furthermore, the EDPS has concerns on the implications of the double status of AMEX for the data subjects' rights. In cases where AMEX is acting as a processor, EFSA must ensure that the data subjects' rights to access, correct and have data erased are fully implemented by AMEX. Specific procedures should be agreed upon between EFSA and AMEX regarding the modalities for the exercise of data subjects' rights. Furthermore, EFSA must ensure that it provides EFSA staff and external experts with appropriate information about the data processing, in accordance with Articles 11 and 12 of the Regulation.

3.4. Onward data transfers by AMEX

As described in section 2.4 above, AMEX further transfers data concerning EFSA staff and external experts to external recipients, including AMEX's suppliers and affiliated companies for purpose of making travel arrangements and third parties for purpose of making reservations, producing reports, collecting payments, and auditing AMEX services upon request from EFSA.

The EDPS notes that with respect to these categories of external recipients there is no indication in the Covenant as to whether these transfers are only made to recipients within EU/EEA countries or internationally to countries outside the EU.

Further, it is not clear what is the legal basis under which all these data transfers take place nor what are the guarantees applied by AMEX for transferring data to external recipients when they are located outside the EU in countries that are not deemed to ensure an adequate level of data protection.

In cases where AMEX acts as a data controller, the EDPS emphasizes that such onward data transfers should only occur if they comply with the requirements set forth in Articles 25 and 26 of Directive 95/46/EC. The necessity of these transfers and their compliance with the Directive's requirements should be assessed on a case-by-case basis.

When AMEX acts on behalf of EFSA as a processor and wishes to appoint a sub-processor, the Covenant only foresees that in case of sub-processing in a third country, *"[AMEX] will seek the consent of [EFSA] and will enter into a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on AMEX under these Clauses*". There is however no definition in the Covenant of what "these Clauses" refer to.

The EDPS underlines that data transfers by a EU institution or agency to a processor and/or sub-processor located in a country that does not ensure an adequate level of data protection may only take place within the frame of Article 9 of the Regulation. It should be verified, on a case-by-case basis, whether a transfer could legitimately take

place under one of the grounds listed in Article 9(6) of the Regulation, for example because the data subject gave his express consent (Article 9(6)(a)) or because the transfer is necessary for the performance of a contract entered into in the interest of the data subject (Article 9(6)(c)).

Without prejudice to Article 9(6), and depending on the circumstances of the case, additional data protection safeguards may be required for the transfer to take place. Such safeguards may result from appropriate contractual clauses (Article (9(7)). In this view, the EDPS notes that the Data Protection Covenant is not based upon the standard contractual clauses approved by the European Commission. In itself, such Covenant does not provide for sufficient safeguards in order to transfer data outside the EU. In particular the EDPS notes that under the Covenant the data importer has very minimal obligations: there are no third party rights; clauses on applicable law, on liability and on resolution of disputes have been omitted; and furthermore there is no detailed description of the data transfers taking place (contrary to what would be required in Appendix B of the standard contractual clauses).

The EDPS therefore strongly recommends that EFSA ensures that appropriate safeguards are put in place for data transfers by AMEX, acting as processor, to its sub-processors located outside the EU and that it receives appropriate guarantees as to the safeguards implemented in respect of onward transfers from AMEX, acting as data controller, to recipients located outside the EU.

4. Conclusions

On the basis of the preceding considerations, the EDPS concludes that a number of processing operations undertaken or envisaged by EFSA for purpose of using the travel services of AMEX are or would be in violation of Regulation (EC) No 45/2001. In particular, the EDPS finds that:

- any further processing by EFSA of data processed in the DoI database for purpose of providing AMEX with travellers' identification data would be in violation of Article 4(1)(b) of the Regulation;

- the potential transfers of all potential travellers' identification data and the current transfers of travellers mission specific data do not meet the conditions of Article 8(b) and Article 4(1)(c) of the Regulation;

- the responsibilities of AMEX in respect of the data processing and the data protection safeguards that it should apply are not sufficiently made clear in the Covenant, which should notably provide clear justification on the role of AMEX as processor and/or as controller and specify the modalities for ensuring the exercise of their rights by data subjects;

- EFSA should provide an appropriate data protection notice to EFSA staff and external experts about the data processing undertaken in relation to the use of AMEX services, in accordance with Articles 11 and 12 of the Regulation;

- EFSA should ensure that the conditions of Article 9 of the Regulation are met in order for AMEX, acting as processor, to transfer EFSA staff and external

experts' data onward to sub-processors located in countries outside the EU. EFSA should furthermore ensure that it receives appropriate guarantees, on a case-by-case basis, as to the safeguards implemented in respect of onward transfers from AMEX, acting as data controller, to recipients located outside the EU.

The EDPS therefore recommends EFSA to adopt the necessary measures to ensure compliance with Regulation (EC) 45/2001 in the light of the conclusions above, and subsequently provide him within two months with all relevant documents evidencing proper implementation.

Done in Brussels, on 21 December 2010