# Europol Joint Supervisory Body

# Data Protection Inspection Report

# September 2014

**Report No. JSB/Ins.14/41**

**Brussels, 9 December 2014**

CONTENTS

**I. INTRODUCTION** ..... 3

***General*** ..... 3

***Scope of the inspection*** ..... 3

***Methodology*** ..... 4

**II. REPORT** ..... 6

**A. Request of the European Parliament** ..... 6

**B. Europol and Information** ..... 6

**B.1 Sending personal data to Europol** ..... 7

**B.2. Dissemination of personal data by Europol** ..... 9

**B.3. Europol's data processing** ..... 10

**B.4. Europol's data protection responsibilities** ..... 11

**C. The inspection** ..... 13

**C1 Findings** ..... 13

**C2 Evaluation** ..... 16

**VI. Glossary / Acronyms** ..... 17

**ANNEX** ..... 18

# I. INTRODUCTION

## *General*

On 21 February 2014, the European Parliament adopted a resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs[1].

In this resolution, based on a report of the Committee on Civil Liberties, Justice and Home Affairs, many concerns are raised following the revelations of Mr. Edward Snowden. In that resolution, the European Parliament calls on the Europol Joint Supervisory Body (JSB)[2], together with national data protection authorities " *to conduct a joint inspection before the end of 2014 in order to ascertain whether information and personal data shared with Europol have been lawfully acquired by national authorities, particularly if the information or data were initially acquired by intelligence services in the EU or a third country, and whether appropriate measures are in place to prevent the use and further dissemination of such information or data; considers that Europol should not process any information or data which were obtained in violation of fundamental rights which would be protected under the Charter of Fundamental Rights;"* [3]

The JSB being composed of representatives of the national data protection authorities making it possible to use the national experiences of its members, decided in its meeting on 19 March 2014, to answer to this call of the European Parliament. Following that decision, the JSB adopted the scope of the inspection of Europol and mandated an inspection team[4] in its meeting on 16 June 2014. On the same date, the JSB informed the Director of Europol that an inspection would take place in September.

The JSB was rendered every service it needed in preparing and conducting the inspection.

## *Scope of the inspection*

Some issues referred to in point 84 of the Resolution, are only related to national activities and will not be part of the scope of the present inspection.

The main issue addressed in point 84 of the Resolution is to ascertain whether data, that has not been lawfully acquired, are processed by Europol. This is directly related to the standard of data

1 (2013/2188(INI))

2 Established by Council Decision (2009/371/JHA) of 6 April 2009, establishing the European Police Office (Europol), OJ.L 121, 15.5.2009, p. 37

3 Point 84 of the Resolution(2013/2188(INI))

4 See annex I

protection Europol has to take into account[5]. Europol must observe the principles of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981(ETS No 108) and of Recommendation No R(87) of the Committee of Ministers of the Council of Europe of 17 September 1987. Basic data protection principle underlined in these instruments is that data shall be obtained fairly and lawfully[6]:
In view of this, the scope of the inspection will be describing the allocation of data responsibilities of the different actors involved in the data processing by Europol and to check data processed by Europol to establish whether these data were unlawfully obtained by the party transmitting these data to Europol.

### *Methodology*

Under Article 34(1) of the Europol Council Decision (ECD), the Europol Joint Supervisory Body (JSB) is tasked with reviewing Europol's activities in order to ensure that the rights of the individual are not violated by the storage, processing and use of data held by Europol.

The JSB seeks to ensure that Europol processes personal data in accordance with relevant data protection principles; namely, the relevant provisions of the ECD together with the principles of the Council of Europe Convention of 28 January 1981 and of Recommendation No R(87)15 of the Committee of Ministers of the Council of Europe. In view of the Resolution of the European Parliament, this inspection report describes all relevant responsibilities for data processing by Europol and the responsibilities of those contributing to that data processing. In addition, the content of the Analytical Work File Counter Terrorism and the content of the Europol Information System are checked. Where necessary, the messages exchanged between Europol and Member States or third States or international organisations will also be checked.
When checking the content of the various systems, the JSB assessed whether there are indications that data were obtained in such a way that there might be doubt whether it was done in compliance with national law (Member States' or third parties) or the legal framework of an organisation (Interpol, Eurojust). This included checking whether there might be indications that the way the data were obtained, or the source they were obtained from, might not be in compliance with national or international law. Data were checked that were transmitted by Member States and by third parties. This included contributions from states or parties for investigations in which they are not participating.
This report must be a public one in view of the issues at stake and will thus not contain information on specific persons or cases that were investigated.

[5] See Article 27 Europol Council Decision
[6] See Article 5 (a) of Council of Europe Convention (ETS No 108) of 28 January 1981

The draft inspection report was submitted for comments to Europol on 8 October 2014. Europol's positive reaction was received on 24 October 2014.

This report has been drafted in only one language - English.

## II. REPORT

### A. Request of the European Parliament

When analysing point 84 of the Resolution, a distinction should be made between the following questions/elements:

*i) to ascertain whether information and personal data shared with Europol have been lawfully acquired by national authorities,*
*ii) particularly if the information or data were initially acquired by intelligence services in the EU or a third country,*
*iii) whether appropriate measures are in place to prevent the use and further dissemination of such information or data;*
*iv) Europol should not process any information or data which were obtained in violation of fundamental rights which would be protected under the Charter of Fundamental Rights.*

Points i) and ii) fall exclusively under national competences and cannot be included in the JSB's inspection. It is up to the national authorities, including the national data protection authorities, to deal with these issues.
Point iii) is applicable both on national and on Europol level.
Point iv) only regards Europol activities.

This report focuses on the implications of the rules on dissemination of information to Europol and the dissemination by Europol (point iii) and the obligation of Europol not to process any information or data which were obtained in violation of fundamental rights which should be protected under the Charter of Fundamental Rights (point iv).

### B. Europol and Information

The ECD provides for specific rules on the transmission of personal data to Europol, the processing of these data and its transmission by Europol. For a better understanding on the various roles of the different actors involved in the transmission to and from Europol and the data processing at Europol, a short overview of these actors and roles will be presented. This overview is also important for establishing the various responsibilities for the data processing.

## B.1 Sending personal data to Europol

*From Member States.*

Europol can process personal data only when it receives data. In view of the objective of Europol to support and strengthen action by competent authorities of the Member States, most data it processes is transmitted to Europol by law enforcement authorities[7] of the Member States. The ECD structures and channels this transmission of personal data to Europol by the creation of Europol national units[8] and the obligation for each Member State to second a liaison officer to Europol[9].

Connected to the structuring of the exchange of information is the allocation of responsibilities for the information exchanged. According to Article 8(4)(g) ECD, the national units shall *"ensure compliance with the law in every exchange of information between themselves and Europol".*

Article 29(1)(a) ECD contains a more general description of and allocates the responsibility "*as regards to the legality of the collection, the transmission to Europol and the input of data, as well as their accuracy, their up-to-date nature and verification of the storage time limits of data"* to the Member State *"which input or otherwise communicated the data".*

Furthermore and according to Article 29(2) ECD, data that has been transmitted to Europol but not inputted yet in one of Europol's data files shall remain under the responsibility of the Member States transmitting those data. When a Member State transmits data to Europol for inclusion in one of the analytical work files, the transmitting Member State should notify Europol for which purpose these data were transmitted;

The general rule is evident: the Member State is responsible that the data it is transmitting to Europol (sending it or directly inputting it in Europol's data files) is obtained (collected) in compliance with the law.

The concept of "the law" in Article 8(4)(g) ECD in connection with the responsibilities as defined in Article 29 ECD refers to the national law of the Member States and the provisions of the ECD. E.g. when a Member State is automatically inputting data in the EIS, the provisions defining the content of the EIS and the definition of the competence of Europol should be checked and complied with together with the national laws[10].

---

7 Data exchange takes in principal place via the national unit, see in this respect Article 8(2) Europol Council Decision

8 See Article 8, Europol Council Decision

9 See Article 9, Europol Council Decision

10 See in this respect also the JSB report 12-61 on the conditions for Europol National Units in relation to data processing in Europol's Information System; http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en

Europol may also receive personal data from Member States when it participates in joint investigation teams[11]. This active participation in investigations does not change the allocation of responsibilities.

*From third parties.*

Europol may receive personal data from others than the Member States. Chapter IV of the ECD regulates Europol's relations with partners. The following groups of partners may transmit personal data to Europol:

- Union or Community institutions, bodies, offices and agencies[12];
- third States and organisations[13];
- private parties and private persons[14].

When a third party transmits data to Europol for inclusion in one of the analytical work files, the transmitting party should notify Europol for which purpose these data were transmitted;

Article 21 ECD creates the possibility for Europol to have direct access to other information systems. This is only possible when Union, international or national legal instruments so allow. The most known system to which Europol has access is the Schengen Information System[15].

According to Article 29 (1) (b) ECD, the responsibility for the data received from a third party will be for the receiving party. Europol is responsible for *the collection, the transmission to Europol and the input of data, as well as their accuracy, their up-to-date nature and verification of the storage time limits of data".*

In practice, Europol ensures compliance with the principle of lawful collection of data in the legal instruments necessary for the exchange of information with third parties.

For example, Europol may only exchange personal data with third States when an operational agreement is concluded[16]. The model used for most agreements contains in the chapter General provisions concerning the exchange of information, the standard clause that:

***"(xxx)** shall only supply information to Europol that was collected, stored and transmitted in accordance with its national legislation. In this context Europol will in particular be bound by Article 4 (4) of the Council Act of 3 November 1998 laying down rules concerning the receipt of information by Europol."*

---

11 See Article 6, Europol Council Decision
12 See Article 22, Europol Council Decision
13 See Article 23, Europol Council Decision
14 See Article 25, Europol Council Decision
15 See Article 41, Council Decision 2007/533/JHA, OJ.L 205, 7.8.2007, p. 63
16 See Article 23(2), Europol Council Decision. Article 23(9) introduces an exemption to the rule that an agreement should be in place.

Presently the following provision is included:
*"Parties shall only supply information to each other which was collected, stored and transmitted in accordance with their respective legal framework and has not been manifestly obtained in violation of human rights."*
In situations where national legislation is not applicable, a reference to principles to be protected is introduced. The agreement with Interpol contains the following provision:
*"In accordance with its respective legal framework neither Party may process information which has clearly been obtained in obvious violation of human rights".*

The cooperation with Union or Community institutions, bodies, offices and agencies as far as it regards the exchange of personal data is limited to Eurojust. The cooperation agreement with that agency does not contain a specific article relating to violations of human rights. Such a provision is not necessary since the rule of law and the general data protection principles apply to all these institutions, bodies, offices and agencies.

When Europol has access to other systems, the legal framework of these systems need to contain specific rules on responsibilities of data[17] holding a Member State responsible that data are lawfully inputted.

### B.2. Transmission of personal data by Europol

In view of Europol's objective to strengthen action by the competent authorities of the Member States, most of the transmission of data processed at Europol will be directed to law enforcement authorities in the Member States. Dependant on the type of information processing system in which the data are processed, a different system of transmission of information by Europol will be applicable.
According to Article 13 (1) ECD, regulating the access and use of EIS, national units and liaison officers of the Member States may retrieve data directly from the EIS. Competent authorities designated by the Member States can also query the EIS[18].

For the analytical work files, a more specific regime applies. Following the structures of analytical work files and analytical groups, only the participants of an analysis group may retrieve data. Participants are those Member States supplying the information or concerned by the analysis[19].
To what extent such retrieval might take place and any possible conditions and restrictions shall be decided upon by the participants of an analysis group.

[17] See Article 49 (1), Council Decision 2007/533/JHA establishing SIS II.
[18] See Article 13(6), Europol Council Decision
[19] See in this respect Article 14 (2 and 4), Europol Council Decision

A specific search function is available for duly empowered Europol staff, liaison officers and duly empowered members of the national units. This "Index function"[20] only allows to establish whether a certain item is processed in an analytical work file.
Europol may further invite experts from third parties to be associated with the analytical work. Such possibility is limited to the parties referred to in Articles 22 and 23 ECD and further conditioned by Council decision 2009/934/JHA, containing implementing rules for Europol's relations with third parties. Private parties and private persons are excluded[21].

Transmission of data may be restricted by the state or organisation that communicated the data to Europol. Article 19 of the ECD allows the use of particular restrictions of the use of data including the transmission of data.

Article 24 ECD contains the general rule that Europol may only transmit personal data received from a Member State to a third party with the consent of that Member State.

### B.3. Europol's data processing

The ECD describes two types of data processing systems that Europol should establish or facilitate: the Europol Information System[22] and analytical work files[23]. It furthermore creates a basis for Europol to process personal data for determining whether such data are relevant to its tasks and can be included in one of the systems described[24]. The ECD also contains a flexibility instrument in Article 10(2): Europol may also establish other data processing systems.
Specific rules for the analytical work files can be found in Council Decision 2009/936/JHA[25].

Apart from these information systems, Europol established a Secure Information Exchange Network Application (SIENA) facilitating the exchange of information between Member States and some third parties with Europol. This system is also used by Member States to exchange information between themselves. All data exchanged using this system are centrally processed by Europol.

[20] See Article 15, Europol Council Decision
[21] OJ.L. 325, 11.12.2009, p.6
[22] See Article 11, Europol Council Decision
[23] See Article 14, Europol Council Decision
[24] See Article 10(4), Europol Council Decision
[25] OJ.L 325, 11.12.2009, p. 14

## B.4. Europol's data protection responsibilities

*General*

Article 29 ECD regulates the responsibilities in data protection matters for data processed at Europol. As already stated in the previous chapters, the general rule is that Member States are responsible for the data they transmit to Europol or directly input in one of Europol's data files. When Europol receives data from third parties, Europol is responsible.

*Europol Information System*

As already described in chapter B 1, Member States are responsible for the data they directly input in the EIS or for the data they send to Europol for inputting in the EIS.

Europol's responsibilities for the exchange of information by using the EIS can be described as follows:

Firstly, Article 11(2) ECD, first sentence, gives Europol a general responsibility to ensure compliance with the provisions of the Decision governing operation of the EIS.

Secondly, Europol has an organisational responsibility for technical and operational aspects of the functioning of the EIS.

The responsibility defined in Article 11(2) ECD does not change the responsibility of the Member States for the content of the EIS. It stresses Europol's obligation to have such a system established and that it is used in compliance with the provisions of the ECD. Such responsibility is also laid down in Article 29(3) ECD: *"In addition, subject to other provisions in this Decision, Europol shall be responsible for all data processed by it"*.

A similar provision as in Article 29(3) ECD already existed in the Europol Convention[26]. Article 15 of that convention also made Europol responsible in addition to responsibilities of others. The JSB explained in its Europol inspection report 2006 the consequences of such additional responsibility in relation to the data processing in the Europol Information System as defined in Article 7 Europol Convention:

*"Article 15 thus places a shared responsibility for the content of the EIS to the Member State that puts the data in the information system and Europol. This shared responsibility should be regarded as complementary: a Member State is responsible for the content of its data and Europol has a general obligation to take care that processing of data in the EIS fulfils all conditions for this processing. Such a general obligation will include a policy of informing users of the EIS about its purpose and other conditions for entering data. However, it also includes an obligation to inform a*

[26] OJ.C 316, 27.11.1995, p.2

*Member State that inputted data in the system that there are reasons to believe that the data are incorrect or not necessary for the performance of Europol's task. In view of Europol's facilitating role in respect of the IS, this obligation does not create an obligation to check every data entry of a Member State. It does however create an obligation in those cases where Europol detects data that might be incorrect or not necessary for the purpose of the IS, to inform the Member States of its findings."*

Although this statement of the JSB was made in a specific situation where doubts could be raised on the correctness or necessity of data processed, the responsibility described also includes the lawfulness of obtaining data. When Europol detects that data may not be lawfully obtained, Europol should contact the inputting Member State.

Such an obligation also exists if Europol detects or should have detected that data inputted might not have been lawfully obtained.

When Europol inputs data received from a third party in the EIS, Europol is responsible for "*the legality of the collection, the transmission to Europol and the input of data, as well as their accuracy, their up-to-date nature and verification of the storage time limits of data*"[27]. This responsibility includes a responsibility for the lawful obtaining of the data.

*Analytical work files*

The specific rules for the analytical work files[28] also contain specific provisions indicating who is responsible. According to Article 3(2) of these rules, data shall be subject to the national legislation of the Member State providing the data until such data are included in an analysis work file.

Applying Article 29 ECD and Article 3(2) of Council Decision 2009/936/JHA, Europol is fully responsible for the data it processes in analytical work files.

The practical implementation of Europol's responsibilities for the content of the analytical work files is not always an easy task. The JSB referred to this in its annual 2014 inspection report stressing that Member States have a clear responsibility for the data they send to Europol for inputting in an analytical work file. In that report the JSB refers to a situation "*where the complete content of data bases, hard disks or mobile phones were sent to Europol by Member States without knowing the content. In view of the responsibilities of Member States as defined in Article 29 ECD, simply leaving such an assessment to Europol whether data may be included would not be in line with that responsibility".*

[27] See Article 29(1)(b), Europol Council Decision

[28] Council Decision 2009/936/JHA

*SIENA*

SIENA is a mailing system tailor made to exchange information necessary to fulfil Europol's tasks. It is also used by Member States to exchange information including personal data between themselves.

As already explained in the two opinions on the Europol regulation[29], Europol acts, when facilitating the exchange of information with SIENA, as a service provider.

An important feature of this mailing system is the central storage by Europol of all messages exchanged, including the messages that are not directed to Europol. Messages are processed in separate folders dedicated to each of the SIENA participants. Europol only has access to its own folders containing data sent to Europol; it has no access to the folders containing Member States' data. In so far the messages and their content include personal data, the responsibilities of Article 29 of the ECD come into play. This article regulates the various responsibilities for the data processing by Europol and is written to cover the various forms of data processing described in the ECD. The responsibilities for using SIENA should follow and remain in line with the division of responsibilities as introduced in Article 29 of the ECD

## C. The inspection

During the inspection of the content of Europol's files, the JSB checked:

i) whether data are processed that are obtained in violation of fundamental rights

ii) whether there are indications that data are not obtained in compliance with national law or with legal framework of a third party

iii) whether data referred to under points i) and ii) are exchanged by Europol.

Data checked are data from received from Member States and from third parties. Where considered necessary the SIENA messages related to these data were also checked.

### C1 Findings

The main focus of the inspection was to check the processing of personal data in the AWF Counter-terrorism and to assess whether these data were unlawfully obtained by the parties transmitting data to Europol. In view of Europol's role and responsibilities, the JSB checked whether there are indications that data were obtained in violation of human rights and/or not in compliance with the national law of the sending party.

[29] JSB Opinion 13/31 of 10 June 2013 and JSB Opinion 13/56 of 9 October 2013, published on http://europoljsb.consilium.europa.eu/opinions/others.aspx?lang=en

The AWF Counter-terrorism is divided in several focal points, each focussing on specific types of terrorism. The focal points were inspected except one focal point that was not relevant for this inspection since it only contains information published on websites.
The AWF Counter-terrorism facilitates the processing and analysing personal data and data on international criminal investigations and criminal intelligence operations against specific persons, groups and entities. [30]
The JSB inspection included a check of the operational projects within the AWF Counter-terrorism.
Prior to the inspection, a list of personal data processed in the EIS was given to the JSB. Persons on this list are categorised as suspect or potential suspect of terrorism.

In the inspection, the JSB checked data on persons having one of the following relation to terrorism or a relation with persons suspected of committing terrorism:
1. persons who in accordance with the national law of the MSs are suspected of having committed or having taken part in a terrorist act (suspects)[31];
2. persons who have been convicted of a terrorist act (convicts)[32];
3. persons regarding whom there are factual indications or reasonable grounds under national law to believe that they will commit a terrorist act (potential suspects)[33];
4. persons who have sporadic contact with the persons in 1 and 2 (contacts)[34];
5. persons who have regular contacts with persons in 1 and 2 (associates)[35].

Data of more than hundred and fifty persons were checked. Established terrorist groups and entities were further investigated to evaluate the contributions received from the Member States.
These data were transmitted to Europol by Member States, third States and international organisations.

The inspection included a verification whether the categorisation as suspects, potential suspects etc. was based on sufficient information indicating the type of relation of the person with terrorism. This information could be included in the contribution of the party transmitting the data to Europol. These contributions were also inspected for indications that the data might be obtained in violation of human rights or not in compliance with the national law.
During the inspection, special attention was given to persons processed as potential suspects.

[30] *Council of the European Union regularly updates the list of persons, groups and entities subject to art.2,3 and 4 of Common position 2001/931/CFSP on the application of specific measures to combat terrorism*
[31] *See Article 12 (1) (a) ECD*
[32] *See Article 12 (1) (a) ECD*
[33] *See Article 12 (1) (b) ECD*
[34] *See Article 14 (1) (d) ECD*
[35] *See Article 14 (1) (d) ECD*

A summary of the findings of the check of the data can be divided into two groups:

1. In the inspected cases, the JSB did not find any indication that the data processed might be obtained in violation of human rights or not in compliance with the national law. The data checked complied with Europol's mandate.

2. In most of the cases, the JSB found sufficient information linking the person and the (suspected) terrorist activity. However, in some cases the contributing part did not provide sufficient information reconstructing why a person is regarded as suspect or potential suspect. In practice, Europol receives huge amounts of data, contained in extensive lists of persons. The context in which these data are processed might be clear but it is not always obvious why a contributing party labels a specific person as suspect or potential suspect.
When data are introduced in the EIS by a Member State, that state sometimes inputs only the identification data and the category of crime (terrorism) without further explanation. Sometimes the contributions are lacking explicit information allowing proper assessment because they are parts of a continuously updated chain of information. Another explanation is that the information leading to the processing of personal data in EIS or in the AWF Counter Terrorism is classified higher than EU restricted[36]. The systems in which Europol processes data are accredited for EU restricted and may not process data of a higher security level.

Following several recommendations made by the JSB in the annual inspections held at Europol, the Analysis Work File Manual (Manual) was approved by the Director of Europol on 19 August 2014. This Manual describes the practical functioning of the AWFs and aims to standardise the relevant working processes. The chapter describing the process of assessing and accepting contributions instructs the responsible operational centre to make an assessment "……. *that there is no evidence that the information provided was obtained in violation of fundamental rights.*"
The chapter dealing with the "Ad hoc review" of data instructs to delete data if it becomes evident at any point that data processed within the AWF's has been obtained in violation of fundamental rights.

[36] *art.11, Council Decision 2009/968/ JHA of 30 November 2009 adopting the rules on the confidentiality of Europol information*

## C2 Evaluation

The JSB did not find any information indicating that data was obtained in violation of human rights or not in compliance with the national law of the contributing States or international organisations.
There were some cases in which the JSB did not find sufficient information in the contribution of the transmitter of the data allowing a proper assessment why these data were sent to Europol. This makes it impossible for Europol and the JSB to assess whether there is any indication and whether these data were gathered in compliance with the national law and without violation of the human rights.
In other cases the information about a person or on a certain operation is lacking because of the existence of a classification level that doesn't allow the distribution of the respected information via sources with lower protection level. The JSB stresses that the role of the national units and their responsibility for the information sent (see Chapter B1 of this report) should ensure that Europol is given the opportunity to check the legality of the data.
The JSB notes that Europol has sufficient procedural measures in place to ensure that the incoming data to Europol is checked for compliance with the legal provisions before its input in the system.

## VI. Glossary / Acronyms

**AWF**: Analysis work file as referred to in Art. 14(1) ECD

**AWF CT**: Counter Terrorism

**AWF rules**: Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files

**EAS**: Europol Analysis System

**EIS:** Europol Information System

**ENU:** Europol national unit

**ECD**: Council Decision 2009/371/JHA of 6 April 2009 establishing Europol

**FP**: Focal point

**JSB** Joint Supervisory Body

**RESOLUTION:** resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs

**SIENA**: Secure Information Exchange Network Application

**TG**: Target group

## ANNEX

On 16 June 2014, the JSB mandated the following inspection team to carry out the inspection at Europol on 24-25 September 2014:

Mrs M. Matousova, member of the JSB from the Czech Republic data protection authority (DPA) and coordinator of the inspection team
Mrs C. Guerra, member of the JSB from the Portuguese DPA
Mr M. Garcia Sanchez, member of the JSB from the Spanish DPA
Mr P. Breitbarth, member of the JSB from the Dutch DPA
Mr G. D'Acquisto, expert from the Italian DPA
Mr P. Michael, Data Protection Secretary to the JSB
Ms D. Borisova, assistant to Data Protection Secretary to the JSB