Opinion on a notification for Prior Checking received from the Data Protection Officer of the European External Action Service on security investigations

Brussels, 1 February 2013 (2011-1059)

1. Proceedings

On 21 November 2011, the European Data Protection Supervisor (**EDPS**) received a notification for prior checking from the Data Protection Officer (DPO) of the European External Action Service (EEAS), on security investigations carried out by the Division for Security and Security Policy of the EEAS. The notification was accompanied by a Privacy Policy Statement.

Questions were raised on 20 December 2011 to which the EEAS replied on 14 June 2012. Further requests were made: on 21 June and replied on 23 July and on 9 August with reply on 31 August. In the meantime, a revised notification was sent on 23 July 2012. On 10 September, based on article 27.4 the EDPS extended the deadline for adoption of the prior checking Opinion by two weeks (24 September) which was then further extended until 8 October due to the complexity of the case. Additional requests for information/clarification were made on 8 October (reply 14 December 2012). The EDPS further extended the deadline of one month on 17 December 2012. The draft Opinion was sent to the DPO for comments on 16 January 2013. The EDPS received the reply from the EEAS on 31 January 2013.

2. The facts

2.1 Purposes

Based on the notification, the primary purpose of the processing of the data is the investigation of actual and suspected breaches of security, compromise or loss of EU classified information (EUCI) and security incidents or threats to the EEAS security interests. This general purpose is divided in different processing operations explained here below.

The **controller** is the EEAS, here represented by the Head of Division for HQ Security and EEAS Security Policy.

The legal basis for the processing operations covered by this purpose is composed by the following legal instruments:

1. Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service, Art. 10. 2 on Security (2010/427/EU).

2. Council Decision of 31 March 2011 on the security rules for protecting EU classified information, and in particular Art. 1, 7, 12 and 13 (2011/292/EU)[1].
3. Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 15 June 2011 on the security rules for the European External Action Service, and in particular Art. 1, 7, 8, 9 and 10[2] (2011/C 304/05).
4. EU Commission Decision on 08/09/1994.
5. EU Commission Decision 844 on 29/11/2001[3] and Euratom Regulation n. 3 of 31/07/1958[4].
6. EU Commission Administrative information n. 45/2006 on 15/09/2006.

Moreover, the EEAS was, at the time of the opinion, drafting a consolidated[5] "Decision of the High Representative of the Union for Foreign Affairs and Security Policy [...] on the security rules for the European External Action Service" ("the draft consolidated Decision"). This Decision, as stated by the controller, clarifies the predictable events to be investigated and covers the following events:
- actual or suspected breaches of security (Article 8);
- actual or suspected compromise or loss of EU classified information (EUCI) (Article 8);
- actual or suspected security incidents or threats to the EEAS security interests (Article 2).

Purpose and types of processing activities

Under the general purpose described above, the EEAS' procedure covers various processing activities:

2.1.1) Investigation of security incidents, breaches or threats to EEAS security interests.
Article 9 of the draft consolidated Decision elaborates on the investigation of security incidents, breaches and/or compromise and corrective actions as follows.

Investigations or verifications are allowed to be conducted:
(I) where it is known or where there are reasonable grounds to assume that classified information relevant to EEAS has been compromised or lost,
(II) on any actual or suspected breach of security or any other security incidents or threats to the EEAS security interests.

In case of the aforementioned events, a file is created to collect all elements that can contribute to the manifestation of the truth, to the damage assessment and to the possible identification of the author of the alleged act. This includes the declaration of the complainants, of witnesses, potential perpetrators, but also of any relevant evidence. The goal is to establish a report to be sent, as appropriate, to the authority competent for the case. Article 9 also states that: "*Where access to information relates to private data contained on*

[1] The Decision lays down the basic principles and minimum standards of security for protecting EUCI.
[2] The Decision lays down the rules for the safety and security of the EEAS. It establishes the general regulatory framework for managing effectively the risks to staff, physical assets and information, and for fulfilling its duty of care responsibilities in this regard.
[3] The Commission Decision of 29 November 2001 foresees a structure comprising a Commission Security Office and on the level of the Commission departments, Local Security Officers. In addition, the Decision contains the Commission's provisions on security. Among others, these provisions lay down the basic security principles and standards.
[4] Regulation N. 3 of the Euratom Council of 31 July 1958 determines, among others, the security measures to be applied to information processed by the Community. It also foresees the creation of a security bureau and security officers.
[5] The first rules adopted by the EEAS are defined by the Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 15 June 2011 on the security rules for the European External Action Service (2011/C 304/05).

communication and information systems, such access will be in accordance with Regulation (EC) 45/2001".

2.1.2) Database of cases

It is stated in the notification that a database of cases (open and closed) will be established, including useful information from each folder and allowing both to easily find and to extract certain data, aiming at addressing preventive action and at drawing anonymised statistics. Following information received from the controller, the purpose of the database is to have the kept records supported by an automated tool that allows easy finding/retrieving of files for authorised investigative purposes (search of similar cases, their modus operandi, breach of security repeatedly committed by the same person, facilitating personnel security vetting processes of authorised services, etc).

2.1.3) Access list

Another processing is the establishment, maintenance and updating of a list of people whose access is forbidden in the EEAS premises based on evidence contained in the relevant files. Article 11 of the draft consolidated Decision states that: "Whilst an investigation into the breach and/or compromise is ongoing, the Head of the EEAS Security Directorate may suspend the individual's access to EUCI and to EEAS premises".

This list is established as follows: When an authorized investigation about compromise of EUCI is in process, the authorisation to access EUCI of the person suspected to be responsible for the breach -as per standing rules- may have to be withdrawn by the EEAS Security Authority. As a consequence, the given person's access to EEAS premises (secure areas and/or possibly all premises) shall be denied.

2.1.4) e-monitoring

The EEAS stated in the notification that with regard to research into the specific cases of use of computer and/or communication (such as email, internet, fixed or mobile phones and fax), acceptable use and control measures and investigations are described in the Administrative Information 45/2006 of 15/09/2006 that refers to the rules applicable in the use of ICT services. This Administrative Information relates to e-monitoring of staff activities.

In line with this administrative information, the EEAS clarified that within the framework of the investigation, the anonymity of specific and limited data (traffic and/or content of an electronic mailbox, access to web pages, telephone/mobile phone calls, fax transmissions, etc.) may be lifted.

2.2 Categories of data subjects

Data subjects are all EEAS staff, other agents, contractual agents, former civil servants, service providers, contractors, visitors, third parties spontaneously addressing themselves to the EEAS and to its personnel, i.e. via mail, e-mail, telephone, fax, etc. , or who are victims or witnesses or perpetrators of a breach or an event detrimental to the EEAS interests or its staff.

2.3 Data categories

The data processed in the case of security incidents will depend on the facts ascertained during the investigation. In principle, personal data including surnames, names, possibly place and date of birth, address, the telephone and mobile phones numbers may be processed as well as the nature of the case, its circumstances (when, where, what happened, etc.), the evidence collected and the link between those elements and persons.

The data contained in the database of cases are listed as follows:

number of the file; date of creation of the file; first name/family name/data of birth of the reporting person; name/family name/data of birth of the victim; town of the event; municipality of the event; place of the event; date of the event; part of the day; type of event (possibly by categories); separate field for breach of security; separate field for compromise of EUCI; separate fields for loss of accreditation/parking cards, keys, EEAS pc, mobile or other equipment; brief modus operandi; whether or not reported to the Belgian Federal Police; results of the investigations; field for reporting eventual suspect behaviour/action from persons/cars/staff; actions taken.

The controller stated that personal data which are processed are the data required to allow a search to find the right folder within the database by using keywords. As further clarified by the controller about the search in the database the use of keywords[6] by the EEAS are used to "*find a given case in the future, or to categorise files with the same "modus operandi", or performed in the same place, by the same person, in the same day of the week, etc*". Moreover, all security incidents after they became known and for which a file was created are included in the database.

As to the access list and e-monitoring, the procedure involves consultation of Sysper, Sysper2, Gestel, IOLAN databases, service cards and access entitlements- including photographs -, pensioners, next of kin's files[7], security clearances, consultation, copy and storage of images recorded by camera equipping buildings, queries addressed to DIGIT (email traffic and web logs, phone numbers called from the EEAS premises and buildings where it exercises its activities) based on a defined procedure.

2.4 Data collection and storage

Personal data are processed both manually and automatically in paper and/or digital files. Paper documents are stored in a safe and the electronic files in a secured storage system.

2.5 Transfers of data

Data processed within the processing operation may be disclosed to the following recipients:

- within the EEAS the list of people whose access is forbidden will be disclosed to EEAS officials who need to know in connection with the exercise of their profession activities;

- within other EU institution and bodies to authorised individuals under strict need-to-know conditions (IDOC, OLAF, etc) with their competences;

- within EU member States to authorised individuals or judicial authorities or police, or contracted firms concerned under strict need-to-know conditions;

- to third countries and international organisations pursuant to specific agreements or arrangements for the mutual protection of classified information. The controller clarified that there are third countries and international organisations (IO) with which the EU has stipulated Security of Information Agreements or similar framework. The controller provided the EDPS with an information note of the Council of the European Union on the "Exchange of EU classified information (EUCI) with them ("current version of the EEAS of 22nd of June 2012 - 11766/12"). This note lists the third countries and international organisations with which

[6] As defined by the controller a keyword is any data field listed in the notification that could serve for identification.

[7] Each staff member had to indicate a person whom shall be notified in case of an accident. The name, contact details of the next of kin is kept in personal files by HR department.

such agreements and arrangements exist[8]. All exchanges of information occurring in this context would only concern breaches and/or compromises of security on the handling of classified information that has been shared between the EU (and the EEAS in particular) on the one hand and the third country or IO concerned on the other hand. They will take place under the legal basis of the relevant provisions on collaboration within parties on security investigations in the agreement concerned.

Based on the information provided by the controller, such exchanges will only be made upon a decision on a case-by-case basis, and be subject to verification that the counterpart and the system and procedures in place are trustworthy and that there is an adequate need-to-know from the other part.

In this framework, disclosure of personal data would exclusively be considered in exceptional cases, when

1. Such disclosure is absolutely necessary in collaborating with the third party on the security investigation concerned;
2. The adequacy of the level of protection afforded by the third party has been duly assessed and is considered sufficient in view of the security interest at stake.

If these assessments are positive, the controller states that they would lead to the disclosure of the personal data at stake, on the basis of Article 9.6(d) of the Regulation (EC) No 45/2001.

- It was also specified by the controller that exchange of personal data might be necessary with third countries and international organizations with which there are no such security agreements or arrangements, to protect the EEAS security interests. Here, again, disclosure of personal data would exclusively be considered in exceptional cases, after careful assessment of the adequacy of the level of protection afforded by the third party in relation with:

1. the vital interest of the data subject concerned; or
2. the security interest at stake.

The controller states that if positive, these assessments would lead to the disclosure of the personal data at stake, pursuant to Art. 9.6(e) and/or (d) of the Regulation (EC) No 45/2001 respectively.

Finally, it was stated that for each recipient, the purpose will be to meet obligations deriving from EU Regulations, International Agreements and/or administrative arrangements and national laws, if and when appropriate, to allow tasks covered by the competence of the High Representative of the Union for Foreign Affairs and Security Policy and/or the EEAS to be carried out.

2.6 Conservation of data

The following retention policy applies. Personal data kept in paper and/or digital files as well as in the database may be retained by the administration for a maximum period of ten years from the closing of the file. This period corresponds to the limitations generally accepted by law in connection with penal files. Agents handling the files can be called to testify to the competent bodies.

[8] The list currently in force covers the following states: Australia, Bosnia and Herzegovina, Croatia, Former Yugoslav Republic of Macedonia, Iceland, Israel, Liechtenstein, Montenegro, Norway, Switzerland, Ukraine and United States of America. Other States are involved in negotiations. As to international organizations, it covers: NATO, ICC, ESA. There also exist permanent administrative arrangements with the United Nations.

Personal data contained in the list of people whose access is forbidden in the EEAS premises are kept for the time strictly necessary for the application of the prohibition of access, and in any case not more than five years after implementation of the measure.

2.7 Information to data subjects

A Privacy Policy Statement will be published under the security tab of the EEAS intranet. This document contains information on the identity of the controller, the purpose of security investigation, the legal basis of the processing operation, the data recipients, the existence of the rights of access and rectification, storage period and the right of recourse at any time to the EDPS.

Furthermore, more specific information is provided through different channels, depending on the individuals concerned:

- **Person who is subject of an investigation (person concerned)**

Where it is possible to contact the person concerned, they are informed upon collection of their written statement, which they immediately receive a copy of the policy privacy statement. In other situations, they will be notified at first contact after recording. The EEAS considers that in the case where the notification to the possible person concerned may undermine the investigation, either by the EEAS competent bodies or by judicial authorities, this information is postponed until this is no longer the case.

- **Informants, witnesses and whistleblowers**

The person reporting a fact is automatically notified with the privacy policy statement, if the contact is made by e-mail. If the statement is recorded in writing in the person's presence, a copy of the privacy policy statement is immediately handed over to him/her. If the report is made by phone, the person will be informed orally. The controller states that such phone calls shall be recorded to ensure the authenticity of the report (however, the technical capacity for recording was not yet available at the time of prior-checking analysis).

Witnesses interviewed are notified with the privacy policy statement during the interview and they also get a copy of their statement.

As further explained by the controller, whistleblowing[9] can occur also in the case of security investigations and would be covered under the category of informant. It was further clarified that such cases are covered by Article 8 on security breaches and compromise of classified information of the Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 15 June 2011 on the security rules for the European External Action Service (2011/C 304/05), which states that "any breach or suspected breach of security shall be reported immediately to the EEAS Security Directorate, which shall inform the relevant authorities of the Commission, the General Secretariat of the Council or the Member States as necessary".

[9] According to Article 22 of the Staff Regulation, any official who, in the course of or in connection with the performance of his duties, becomes aware of facts which give rise to a presumption of the existence of possible illegal activity, including fraud or corruption, detrimental to the interests of the Communities, or of conduct relating to the discharge of professional duties which may constitute a serious failure to comply with the obligations of officials of the Communities, shall without delay inform either his immediate superior or his Director-General or, if he considers it useful, the Secretary-General, or the persons in equivalent positions, or the European Anti-Fraud Office (OLAF).

- **People whose access is forbidden in the EEAS premises**

Based on the information received from the controller, the people who are suspects of a security investigation may not be prior informed about their presence in the list due to the fact that it could hamper the investigation procedure. They would be informed if and when they present themselves at an entry point. The controller states that at the end of the investigation procedure, 1) the person would be informed that s/he is forbidden access in the framework of the possible administrative measures taken and 2) if no evidence has been found against the suspect at the end of the investigation, the data of the person will immediately be deleted from the exclusion list. In the controller's view, it is deemed justifiable not to inform the person that s/he had been a suspect, since the person would have not been confronted with the fact that s/he had been under investigation and the investigation would be closed without any consequences for the individual concerned.

2.8 Rights of access and rectification

Data subjects are granted the right to correct the information they have provided, either immediately or subsequently, by making or sending an additional statement which shall be noted to the file. This possibility is always communicated in the interview with the persons concerned, but also exposed in the privacy policy statement available under the security tab of the EEAS intranet.

The controller also stated than when access to data may prejudice the investigation or the rights and freedoms of others, access to these data may be refused, limited or delayed in time on the basis of the exceptions mentioned in Article 20 of Regulation 45/2001. Any data subject can then appeal to the EDPS, who can verify the data relating to him/her and, if necessary, correct or remove them for a legitimate reason.

2.9 Security

[...]

3. Legal analysis

3.1. Prior checking

Applicability of Regulation No 45/2001 ("the Regulation"): Firstly, the processing of data constitutes a processing of personal data ("*any information relating to an identified or identifiable natural person*" - Article 2 (a) of the Regulation). Indeed, as described in the notification, personal data of individuals engaged in the security incident (suspected authors, witnesses, etc) will be collected. Secondly, the personal data collected undergo "automatic and non automatic processing operations", as defined under Article 2 (b) of the Regulation (EC) No 45/2001. For example, in producing a report with information extracted from databases, video surveillance footages, etc. later stored in an electronic database, personal data are processed. Finally, the data processing is performed by an EU body, the EEAS on security investigations in the exercise of its activities falling within the scope of Union law. Therefore, the EDPS considers that all the elements that trigger the application of the Regulation exist in the data processing carried out by the EEAS.

The "draft Decision of the High Representative of the Union for Foreign Affairs and Security Policy on the security rules for the European External Action Service" (**the draft Decision**)

foresees in its article 9(3) that "Where access to information relates to private data contained on communication and information systems, such access will be in accordance with Regulation (CE) 45/2001". The EDPS notes that this limitation of applicability of the Regulation is in conflict with the same Regulation. Indeed, Article 3 of Regulation 45/2001 foresees that "[t]his Regulation shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system". The applicability of Regulation 45/2001 is therefore not limited to processing of personal data by communication and information systems. The draft Decision should be amended in this respect as to reflect it.

Assessment of whether the data processing operations fall under Article 27 of the Regulation. The EDPS considers that data processing clearly falls under the hypothesis foreseen by Article 27.2 of Regulation (EC) No 45/2001.

In the first place, in the EDPS' opinion, such data processing operations fall under Article 27.2(a) of Regulation (EC) No 45/2001, which establishes that processing operations relating to "*suspected offences, offences, criminal convictions or security measures*" shall be subject to prior checking by the EDPS. In the case in point, by carrying out investigations of incidents such as accidents, security breaches, theft, unauthorised access, the EEAS will process information which may relate to alleged offences and crimes and other serious misconduct. This is further confirmed if one takes into account that the final purpose of the processing is the drafting of a report describing the occurrence and eventual transfer to enforcement and judicial authorities.

The controller also submitted the notification under Article 27.2(d), relating to processing operations for the purpose of excluding individuals from a right, benefit or contract. However, the EDPS considers that only the processing intended to exclude people from access to the EEAS premises falls within this article. In his view, the other processing operations covering the creation of a report and the listing in databases do not have by themselves the purpose to exclude individuals from a right, benefit or contract, although this could be a potential consequence. Therefore, Article 27.2(d) only applies to certain processing operations.

The notification of the DPO was received on 21 November 2011. According to Article 27(4) of the Regulation, the present Opinion must be delivered within a period of two months. A revised notification limiting the scope of analysis was sent on 23 July 2012. The procedure was suspended for a total of 297 days to require additional information and 15 days to allow for comments from the controllers. The procedure was also extended for a total of two months due to complexity of the case. Consequently, the present Opinion must be delivered by 1 February 2013.

3.2. Lawfulness of the processing

Personal data may only be processed if legal grounds can be found in Article 5 of Regulation (EC) No 45/2001.

The notification sent by the EEAS foresees Articles 5a, 5b, 5d, 5e of the Regulation as legal grounds. However, of the various grounds listed under Article 5 of Regulation (EC) No 45/2001, the EDPS considers that the processing operation notified for prior checking only falls under Article 5 a), pursuant to which data may be processed if the processing is "*necessary for performance of a task carried out in the public interest on the basis of the*

Treaties establishing the European Communities or other legal instruments adopted on the basis thereof".

In order to determine whether the processing operations comply with Article 5 a) of Regulation (EC) No 45/2001, three elements must be taken into account. First, whether either the Treaty or other legal instruments foresee the data processing operations carried out by the EEAS; second, whether the processing operations are performed in the public interest; and third, whether the processing operations are necessary. Obviously, the three requirements are closely related.

Relevant legal grounds in the Treaty or in other legal instruments. The EDPS takes note of a range of legal instruments, described in the facts, which from a general to a more specific way provide the legal grounds that legitimise processing operations that take place in the context of conducting investigations.

Regarding Council Decision on 26 July 2010 establishing the organisation and functioning of the European External Action Service, Article 10, 2 on Security (2010/427/EU), the EDPS notes that this article foresees that pending adoption of its own security rules in 2011, the EEAS applied the security measures set in the Annex to Decision 2001/264/EC with regard to the protection of classified information and the Commission's Provisions on Security set in the relevant Annex to the Rules of Procedure of the Commission with regard to other aspects of security.

As stated in point 2 above, the controller provided additional information as regards the legal basis by submitting to the EDPS the draft Decision. According to the information received, this consolidated decision should cover the relevant aspects of investigations and replace the legal basis currently used. Among others, Article 9 on investigation of security incidents, breaches and/or compromises and corrective actions and Article 12 on the organisation of security in the EEAS are deemed relevant in the analysis of the lawfulness of the processing.

The EDPS considers that the above legal grounds, from a more general to a more specific perspective, foresee the existence of the EEAS Security Service and its powers as regards the conduct of investigations or verifications. Furthermore, the above legal grounds also generally foresee the kind of processing operations described in the notification. The legal instruments referred to above enable the Security office of the EEAS the carrying out of processing operations towards obtaining information aiming at ensuring secure operating conditions in the EEAS and obtaining information relating to any illegal acts occurring in its departments for the purposes of a judicial inquiry or disciplinary action. From this perspective, the EDPS notes that these legal instruments constitute valid legal grounds to legitimise the data processing operations carried out for the purposes of finding out information related to incidents occurred in the EEAS.

Processing operations are carried out in the public interest. The EDPS notes that the EEAS carries out the processing activities in the legitimate exercise of its official authority. As reflected in the mission statement of the EEAS, this service has the competence and the obligation to engage in investigations for the overall purpose of protecting staff, physical assets and information within the EEAS and in missions established under Title V, Chapter 2 of the TEU. Taking into account the nature of such activities it is clear that they are performed in the public interest insofar as the public interest is served if measures are taken to investigate the authorship of such events and prevent further occurrences in the future.

Necessity test. In order to engage in investigations to find out information about related incidents occurred in the EEAS premises it appears necessary to process personal data. Unless such data are processed it would not be possible for the EEAS to carry out its duties. Thus, from a general perspective, the processing appears necessary for the purposes of performing investigations. This being said, it should be taken into account that the "necessity" of the data processing also has to be analysed *in concreto*, for each particular case, here, for each specific investigation. From this perspective, it has to be borne in mind that the processing of personal data to be conducted in the context of the processing of the information of incidents (as these are described in the facts above) has to be proportional to the general purpose of processing (to ensure the security of the persons, buildings) and to the particular purpose of processing in the context of the case under analysis. Thus, the proportionality has to be evaluated on a case-by-case basis.

3.3. Processing of special categories of data

Taking into account that the purpose of the processing is to facilitate the collection of information about incidents that constitute alleged wrongdoings, it is expected that in a number of cases this information will be related to offences, criminal convictions or security measures. In this regard, the EDPS recalls the application of Article 10.5 of Regulation (EC) No 45/2001 which establishes that *"[p]rocessing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor."* In the present case, processing of the mentioned data is authorised by the legal instruments mentioned in point 3.2 above.

As far as special categories of data are concerned, Article 10.1 of Regulation 45/2001 establishes that "*the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and of data concerning health or sex life, are prohibited*".

From the notification for prior checking it does not appear that data falling under the categories of data referred to in Article 10.1 Regulation 45/2001 are processed in the context of the investigations. Taking into account the overall purpose pursued by the EEAS when it engages in data processing operations, the EDPS understands that the collection of special categories of data is not the EEAS' main goal.

However, the EDPS considers that in the context of the investigation the EEAS may collect and process, perhaps involuntarily, special categories of data. The collection and further processing of sensitive data is admissible only where it is *necessary* in the specific case in view of one of the purposes laid down in Article 10(2). As the processing of sensitive data is to be considered as an exception rather than the rule, the necessity criterion here has to be applied in a restrictive manner.

In this regard, the EDPS recalls the application of the data quality principle (also analysed more specifically below), according to which data must be adequate, relevant and not excessive in relation to the purposes for which collected and/or further processed (Article 4.1.c). Pursuant to this principle, if special categories of data that are clearly not relevant for the purposes of investigating the incident are collected, they should be not be reflected in the written report. Security officers should be made aware of this rule.

3.4. Data Quality

Pursuant to Article 4.1.c of Regulation (EC) No 45/2001, personal data must be *"adequate, relevant and not excessive in relation to the purposes for which collected and/or further processed".* This is referred to as the data quality principle.

Even though certain standard data would be present in the investigation of incidents such as the name, date of birth, address etc, the precise content of a file will of course be variable according to the case. Guarantees must however be established in order to ensure the respect of the principle of data quality. For example, the decision to open an investigation should define the subject and scope of the inquiry. This would help reducing the information collected to what is within the scope of the inquiry. Secondly, the EDPS considers that before investigators start the investigation they must be given instructions quoting Article 4(1)(c) of Regulation (EC) No 45/2001 with a view to encouraging greater caution with respect to collecting evidence or data in an investigation file. Staff called upon to conduct an investigation and draft a report must be given these instructions and must follow them.

According to Article 4.1(d) of the Regulation, personal data must be *"accurate and where necessary kept up to date",* and *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified".*

This principle is very much connected to the exercise of the rights of access, rectification, blocking and erasure (see point 3.7 below).

3.5. Conservation of data/ Data retention

Pursuant to Article 4 (1) e) of Regulation (EC) No 45/2001, personal data may be kept in a form which permits the identification of data subjects for *"no longer than is necessary for the purposes for which the data were collected and/or further processed".*

The EDPS accepts the five year period that applies to personal data contained in the list of people whose access is forbidden in the EEAS premises.

The EDPS also takes note of the ten year period from the closing of the file that applies to personal data kept by the administration in paper and/or digital files as well as in the database.

3.6. Transfer of data

Articles 7, 8 and 9 of Regulation (EC) No 45/2001 set forth certain obligations that apply when controllers transfer personal data to third parties. The rules differ depending on whether the transfer is made *ex* Article 7 to Community institutions or bodies, *ex* Article 8 to recipients subject to Directive 95/46 or to other types of recipients *ex* Article 9.

On the basis of the information provided by the controller, data may be transferred to authorised individuals within the EU institutions and bodies and EU Member States, or judicial authorities or police, or contracted firms concerned, under strict need-to-know conditions. Data could also be transferred to third countries and international organisations pursuant to specific agreements or arrangements for the mutual protection of classified information, should the case arise and involve said third country or international organisation.

Therefore Articles 7, 8 and 9 shall apply and need to be analysed.

Transfer of personal data within or between Community institutions or bodies. The facts described in the notifications for prior checking reveal that data might be transferred to EU institutions and bodies. These bodies are namely OLAF, IDOC, the EDPS or the Ombudsman in the context of their respective competences.

Article 7.1 of the Regulation stipulates: *"Personal data shall only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient"*.

Pursuant to the notification, reports and the related documents (personal data) are transferred to the European institutions and bodies mentioned above only if necessary and on a need to know basis. Given the competences of the recipient bodies, it appears that such data transfers are necessary for the legitimate performance of tasks covered by the competences of the recipients. The proportionality factor has to be considered in this regard, taking into account, for instance, the nature of the data collected and further processed, and the competence of the recipient.

In any case, notice has to be given to the recipient within the EU institution or body in order to inform him/her that personal data can only be processed for the purposes for which they were transmitted.

Transfer of personal data to Member States. Pursuant to the notification, data may be transferred to national law enforcement and judicial agencies. Two scenarios can be observed in Member States: (a) those Member States where the national data protection law adopted for the implementation of Directive 95/46/EC covers every sector of the national legal system, including the judicial sector; and (b) those Member States where the national data protection law adopted for the implementation of Directive 95/46/EC does not cover every sector, and particularly, not the judicial sector. As to the first scenario, Article 8 of the Regulation foresees: *"Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC (a) if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, (...)"*. Thus, even if judicial authorities do not fall within the scope of application of Directive 95/46/EC, if the Member State, when transposing Directive 95/46/EC into internal law, has applied some national implementing rules to these public authorities, Article 8 of the Regulation has to be taken into account. For those countries that have not applied national rules implementing Directive 95/46/EC to judicial authorities, Article 9 of the Regulation applies. In those cases, Council of Europe Convention 108, which for the matter under analysis can be considered as providing a presumption of an adequate level of protection, is in any case applicable to judicial authorities.

Transfer of personal data to third countries and international organisations
For recipients which are not subject to Directive 95/46/EC, Article 9(1) of Regulation 45/2001 provides that "*personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out*". Thus, in principle, data cannot be transferred to recipients in non EEA states which do not provide an adequate level of protection. However, derogations can apply as established under Article 9.6 and 9.7.

Based on the information received from the controller, the EDPS notes that agreements between the European Council and third countries and international organisations on exchanges of classified information have been signed. These agreements are applied by the EEAS as well. Such agreements only foresee the transfers of EUCI information, which may or may not contain personal data. Therefore, for the cases where the EUCI information to be transferred contains personal data, the EDPS invites the EEAS to respect Article 9 of the Regulation.

Furthermore, Article 9 should also be respected in those cases where a transfer would take place to third countries and international organisations with which there are no agreements with the EEAS on the exchange of classified information.

As regards the applicability of Article 9(6) (d) / (e) in such specific cases, the EDPS provisionally accepts the exception being proposed but this decision is taken without prejudice to his conclusion on the analysis of the question in a "position paper on the application of Article 9 of Regulation (EC) 45/2001: transfer of personal data to third countries and international organisations" that is currently being drafted.

3.7. Right of access and rectification

The right of access is the right of the data subject to be informed about any information relating to him or her that is processed by the controller. According to Article 13 of Regulation (EC) No 45/2001, the data subject shall have the right to obtain without constraint from the controller, communication in an intelligible form of the data undergoing the processing and any available information as to their source. The information can then be obtained directly by the data subject or, under certain circumstances, indirectly by the EDPS in the present context.

The privacy policy statement declares that individuals have such rights regarding the information that the EEAS holds about them. It gives a functional email box as the contact person to exercise such rights. The practice as described in the privacy policy statement is generally in line with Article 13 of Regulation (EC) No 45/2001.

Although the privacy policy statement does not foresee the possibility, in certain cases, to defer the obligation to provide access/rectification to safeguard the investigation, this is foreseen in the notification, where it mentions that certain data can be covered by the exceptions mentioned in Article 20 of Regulation 45/2001 (especially under Article 20.1.a and 20.1.c). This could be the case, for example, if the EEAS considers that the disclosure of information may reveal the identity of the whistleblower or informant which may be the case in a number of instances. In deciding whether the EEAS must rely on an exception, it must engage in a case-by-case assessment of the circumstances of the particular data processing at stake.

Furthermore, the right of access is also applicable when a data subject requests access to the file of others, where information relating to him or her would be involved. This would be the case of whistleblowers, informants or witnesses who demand access to the data relating to them included in an investigation conducted on another person. The information can then be obtained directly by the data subject (this is the so-called “direct access”) or, under certain circumstances, by a public authority (this is the so-called “indirect access”, normally exercised by a Data Protection Authority, being the EDPS in the present context).

Moreover, based on the information available from the privacy policy statement and notification, the EDPS considers that in the case of investigations, if the EEAS uses an exception to defer the provision of information, it should take into account that the restrictions to a fundamental right can not be applied systematically. The EEAS must assess in each case whether the conditions for the application of one of the exceptions of Article 20.1.a or Article 20.1.c may apply. In addition, as foreseen in Article 20 of the Regulation, the measure has to be "necessary". This requires that the "necessity test" has to be conducted on a case-by-case basis. If the EEAS uses an exception, it must comply with Article 20.3 according to which *"the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor*". However, the EEAS may avail itself of Article 20.5 to defer the provision of this information as set forth in this Article: *"Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect"*.

In the light of this, and contrary to what is stated in the EEAS notification, only temporary deferrals are allowed. The EEAS can not definitely "refuse" the access to the data. Therefore the word "refuse" should be deleted from the privacy policy statement.

In addition to the above, due account should be taken of the fact that the fair processing of personal data in an investigation and subsequent legal proceedings implies the exercise of the right of defence. In order to exercise that right, the data subject must normally be in a position to know when proceedings have been initiated against him. Any exceptions must therefore be strictly limited and applied on a case-by-case basis.

3.8. Information to the data subject

The Regulation states that the data subject must be informed where his or her personal data are being collected and lists a number of obligatory points to be included in the information, in order to ensure the fairness of the processing of personal data. In the case at hand, the data could be collected directly from the data subject and could also be collected indirectly, for instance, through informants.

It has to be taken into account that all the requisites mentioned in paragraph 1 of Articles 11 and 12 must be complied with, including sub-paragraph f), since, given the sensitivity of the cases that would normally be dealt in the context of the processing activities being analysed, the data subjects must have knowledge of all the guarantees they are entitled to.

In assessing whether the controller for the case in point provides information to individuals, one must address two issues: First, the extent to which the information is effectively provided and, second, the extent to which the content of the information provided, is in line with Regulation (EC) No 45/2001.

The communication channel: According to the notification, the information channel through which individuals are informed is through a privacy policy statement published under the security tab of the EEAS intranet. In addition, according to the notification, individuals, including the person reporting a fact, the persons concerned, witnes(ses) or whistleblower(s), in cases of written and oral declarations are automatically notified of the privacy policy statement, in writing or verbally. *A fortiori*, this will not be the case when such individuals are not interviewed or do not give written declarations[10].

[10] As stated in the notification, if the person(s) concerned can not be contacted, he/she (they) will be notified at first contact after recording.

The EDPS considers that the publication on the Intranet of the Security tab of the EEAS is a positive practice towards informing individuals. But this can not be considered sufficient in the present case. Therefore, the EDPS recommends that the EEAS adopts a procedure to individually provide the privacy policy statement to the data subjects about whom personal data are collected.

As far as informants, witnesses and whistleblowers are concerned, the EDPS recommends that the provision of information is also provided individually, irrespectively of the fact that they are interviewed or not.

However, the EDPS notes that if the EEAS receives information through phone calls, it is foreseen that these shall be recorded to ensure the authenticity of the report. Although not in place at the time of this opinion, this technical possibility is foreseen in the notification. In such case, individuals must also be informed that the recording is taking place. Nevertheless, this is not mentioned in the information provided to the EDPS. The EDPS invites the EEAS to take appropriate measures towards the correct information of the data subjects whose calls may be recorded.

As to the applicability of Article 20 of the Regulation enabling the EEAS to defer the provision of information, the EDPS refers to his comments made above in the context of right of access and on the fact that the restriction to a fundamental right can not be applied systematically. In such case, the EEAS must engage in a case-by-case assessment of the circumstances of the particular data processing at stake

Finally, if the EEAS uses an exception, it must comply with Article 20.3 according to which *"the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor*". However, the EEAS may avail itself of Article 20.5 to defer the provision of this information as set forth in this Article: *"Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect"* (paragraph 3 foresees the right of the data subject to be informed of the reasons why a restriction has been imposed as well as his right to have a recourse to the EDPS; paragraph 4 foresees the indirect right of access to be conducted by the EDPS and the information of its results to be provided to the data subject).

As a consequence, the EDPS does not share the view of the EEAS regarding the non provision of information to the person concerned when no evidence has been found against the suspect at the end of the investigation. Therefore, following the above reasoning, the EDPS can not accept the statement of the EEAS following which *"[I]t is deemed justifiable not to inform the person that s/he had been a suspect, since the person would have not been confronted with the fact that s/he had been under investigation and the investigation would be closed without any consequences for the individual concerned*".

Applying such procedure without informing the data subject at all would be contrary to the Regulation 45/2001 and the right of information of the data subjects with regards to a processing of personal data conducted by the institution and may eventually conduct to complaints against the institution. The EEAS must therefore amend this aspect of its procedure.

The content of the privacy policy statement: the notification, under the header on information to be given to data subjects and means of communicating this information, states that the "existence of the databases and the process to make the data contained checked by the EDPS and, if necessary, to correct them if they prove incorrect, is subject to a statement published under the security tab of the EEAS intranet". The EDPS considers that this wording is incomplete in relation to the requisites of Articles 11 and 12. Therefore, the wording should be amended to reflect this situation.

The EDPS has also checked the content of the information provided in the privacy policy statement and considers that for the most part it contains the information required under Article 11 and 12 of Regulation (EC) No 45/2001. Indeed, it contains information on the identity of the controller, the recipients of the data, the existence of a right of access and the right to rectify, including the name of the contact person to exercise such rights. It also contains the right to have recourse at the European Data Protection Supervisor. The EDPS however considers that the description of the time limits for storing the data should be completed with the time limits that apply to reports that neither result in an effective applicable measure nor are handed to the national enforcement authorities. Therefore, he calls upon the EEAS to complete the privacy policy statement in this regard (see point 3.5 above). Moreover, the EDPS considers that the purpose should be further described. Indeed, the current statement only reads that "The purpose of this processing operation is to perform security investigations".

3.9. Confidentiality of communications

Article 36 of the Regulation stipulates that *"Community institutions and bodies shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the general principles of Community law"*. The concept of "general principles of Community law" refers to the notion of fundamental human rights notably as laid down in the European Convention on Human Rights. Any restriction to the confidentiality of communications must comply then with Article 8.2 of the said instrument: *"[t]here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"*.

This provision has to be respected while conducting e-monitoring, especially as concerns the examination of e-mails. The EEAS refers to the Commission Administrative Information 45/2006 of 15/09/2006 that is applied by the EEAS. Referring to the Commission Administrative Information does not clarify however whether the EEAS would be conducting itself the "research" or, as stated in the information notice, if this task would also be conducted by the services of the Commission IDOC. Furthermore, the draft consolidated Decision that was provided to the EDPS only clarifies that it is the EEAS Security Directorate which conducts the investigations or verifications and implements any necessary corrective actions resulting from investigations[11].

[11] Article 9 of the draft Decision precisely states:

1. The EEAS Security Directorate assisted by experts from Member States and/or from other EU institutions as appropriate, and upon authorisation from the Chief Operating Officer as necessary, shall:

(a) conduct investigations or verifications, as appropriate:

(i) where it is known or where there are reasonable grounds to assume that classified information relevant to EEAS has been compromised or lost;

(ii) on any actual or suspected breach of security or other security incidents or threats to the EEAS security interests;

Therefore, the EDPS invites the EEAS to specifically adopt a procedure covering e-monitoring that may be conducted.

In any case, after considering the requisites contained in Article 8.2 of the European Convention on Human Rights and Fundamental Freedoms, the restrictions to the principle of confidentiality will therefore have to be examined according to the following criteria[12]:

- Is the restriction authorised by a legal provision or equivalent measure?

- Is it necessary? Could the same result be obtained without breaching the principle of confidentiality? It would only be in exceptional circumstances that the monitoring of an agent's personal use of the e-mail (apart from scanning viruses) or internet would be considered as necessary.

- Is it proportionate to the concerns it tries to ally? The principle of proportionality implies that the application of the restrictions to the confidentiality of communications will be different if we are in the case of personal communications or business communications. It also implies that if it is necessary to check the e-mail accounts of workers in their absence, this should in principle be limited to e-mails that are not marked as private or personal or that are addressed to the address of the institution.

As to e-monitoring, the EDPS is currently drafting guidelines covering the processing of electronic communications data by European institutions and bodies.

3.9. Security measures

According to Articles 22 and 23 of Regulation (EC) No 45/2001, the controller must implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. These security measures must in particular prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing.

[...]

The EDPS has no reason to believe that the EEAS has not implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected and that are in line with the measures established in the other EU institutions.

Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 provided the considerations in this Opinion are fully taken into account. In particular, the EEAS must be aware of the following:

(b) implement any necessary corrective actions resulting from investigations, when and as appropriate.

2. Investigators shall have access to all information necessary for the conduct of such investigations and shall receive the full support of all EEAS services in this regard.

Investigators may take appropriate actions to safeguard the trail of evidence in a manner that is proportionate to the seriousness of the matter under investigation.

[12] It should be noted in this regard that the issue of monitoring or inspecting electronic communications (e-monitoring) will be dealt with by the EDPS separately, in horizontal guidelines.

- The EEAS should modify the draft Decision of the High Representative of the Union for Foreign Affairs and Security Policy on the security rules for the European External Action Service when describing the scope of the applicability of Regulation 45/2001 that is currently mentioned in its Article 9;
- It must be ensured that only data that are relevant for the purposes of the investigation are collected and reflected in the written report. Particular attention must be given to special categories of data. Security officers in charge of performing investigations and drafting reports should be made aware of this;
- When data are transferred within EU institutions and bodies and also to national (police and judicial) authorities as well as to third countries and international organisations a notice should be given to the recipients of the data informing them that the data can only be processed for the purpose for which they were transmitted;
- When data are transferred, it should be ensured that this only happens when the transfer is necessary. This necessity should be confirmed in a reasoned opinion;
- The EEAS should document the procedures in case of transfer of personal data to third countries or international organisations covered by EUCI agreements. The EDPS reserves the right to clarify his position as to these transfers, once his policy paper on transfer is adopted;
- The EEAS should adopt procedures to inform the various categories of data subjects, to take appropriate measures as to the content of the information provided and to amend its notification in the light of the comments above;
- The privacy policy statement should be amended as suggested under various points of this Opinion.
- [...]

Done at Brussels, 1 February 2013

(**signed**)

Giovanni BUTTARELLI