Opinion on a notification for Prior Checking received from the Data Protection Officer of the Commission on the Security Investigations at Joint Research Centre ISPRA

Brussels, 31 July 2008 (Case 2007-507)

1. Proceedings

On 3 September 2007, the European Data Protection Supervisor (hereinafter "EDPS") received from the Data Protection Officer of the Commission ("DPO") a notification for prior checking regarding the processing operations carried out in the context of performing security investigations at the DG Joint Research Centre in Ispra ("JRC Ispra").

On 28 September 2007 the EDPS requested from JRC Ispra complementary information. Throughout May and June 2008, the EDPS received, in the context of other prior checks[1], answers to most of the questions addressed to JRC Ispra in his earlier request of 28 September 2007, which enabled the EDPS to finalise a first draft Opinion. On 3 July 2008 the EDPS sent the Draft Opinion to the DPO for comments and to clarify some outstanding factual issues. The feed back was received on 22 July 2008

2. Examination of the matter

Within JRC Ispra the Unit C 7 is responsible, among others, for the security of persons, premises and information of JRS Ispra ("JRC Ispra C7"). Within this Unit, the Security Service ("SeS") implements the policies and procedures set up for the purpose of ensuring the overall security of JRC Ispra. In particular, the SeS is responsible, among others, for the protection of persons, premises and information pertaining to the Commission at the JRC Ispra site against unauthorised access, intrusion and other attacks. In order to carry out this duty, the SeS performs investigations related to security related incidents such as traffic accidents, vandalism theft, unauthorised access, etc. in the context of which personal data are processed. The outcome of the investigation is reflected in a report describing the occurrence. In case of security breaches SeS limits the damage, safeguards evidence and informs Security Directorate, who will decide how to proceed with the investigation.

This prior check analyses whether the data processing carried out by the SeS in the context of performing security investigations and drafting the reports mentioned above is in line with Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter "Regulation (EC) No 45/2001"). This prior check does not analyse the

[1] Notification for prior checking received from the Data Protection Officer of the European Commission regarding the database ARDOS, (Case 2007/380) and notification for prior checking received from the Data Protection Officer of the European Commission regarding security investigations carried out by DG ADMIN, (Case 2007-736)

compliance with data protection in the context of the proceedings that may take place following the drafting of the report.

2.1 The Facts

The ***purpose of the processing*** is to obtain information related to incidents such as accidents, security breaches, theft, unauthorised access, etc. that has occurred in JRC Ispra premises with the final purpose of drafting a report describing the occurrence. The report aims at identifying the authors of such acts, limiting and quantifying eventual damages.

The JRC Ispra Site Director or the Director General of JRC can decide to ban a person from a JRC site as a consequence of the report evidencing a wrongdoing. This is communicated to the individual and to SeS by a letter signed by the authority which took the decision.

The ***primary responsibility for the data processing*** lies with the Unit C7 of JRC Ispra responsible, among others, for security operations of JRC Ispra. In particular, within this Unit, the data controller responsible for the data processing that takes place in the context of running the security investigations is the head of sector who is competent for ensuring the overall direction of the activities of Security Service ("SeS") of JRC Ispra. Most of the data processing operations carried out while running security investigations are performed by the SeS.

In the context of running security investigations, the ***automated*** **and** ***manual*** **data processing operations** are interrelated. When an incident has occurred, a paper dossier is produced which includes complaints, testimonies, declarations and proof elements, such as photographs. In addition, the paper dossier is completed with information extracted from various databases like SECPAC and ARDOS, video surveillance footages and other information that may be useful. At the end, the report will contain the main conclusions of the investigation. The report will be stored both in paper and also in the database ARDOS[2].

The data processing involves the following ***types of data subjects***: *(i)* Any person who is subject to an investigation and *(ii)* individuals who cooperate with the investigation, for example, witnesses or other type of collaborators.

These data subjects may be either staff of the JRC Ispra or third parties. Staff of the JRC Ispra includes active staff such as officials, temporary or contractual agents and also external staff working under a contract. They may also be retired officials. Third parties include visitors or any other person that addresses himself/herself to the JRC Ispra C7. Among others, this may include individuals who contact the SeS by email, telephone, fax, etc. because they are victims, witnesses or authors in a security related incident.

Regarding the categories of personal data, the personal data collected include, on the one hand, information about the incident. This may comprise, depending on the case at stake, a description of the incident, the location, the time and date, as well as supporting evidence such as photographs, video surveillance footage, etc. On the other hand, information about the individual alleged to have committed or who is otherwise involved in the security incident is also included. Such information may comprise the name, date and place of birth, nationality, gender, type of contract, work contact details, type of entry permit into the premises, including start and ending dates, private address, telephone and email address.

[2] A notification for prior checking received from the Data Protection Officer of the European Commission regarding the database ARDOS, is being worked on (Case 2007/380).

The sources of the information are multiple, including the content of various databases such as ARDOS and SECPAC. Information is also collected from video surveillance, from witnesses and other collaborators as well as from the suspected individual.

Conservation periods vary depending on the outcome of the investigation. The information regarding cases that result in effective applicable measures, such as interdiction in accessing a site or a particular area is kept until the applicable measure has to be enforced. The maximum retention period during which this information is kept is five years.

Security investigation reports and related information resulting in a dossier that is handled under criminal law are kept for a maximum of ten years, starting from the conclusion date of the investigation.

Reports which lead to the conclusion that it was not wrongdoing or that it resulted in no effective applicable measure are kept for 12 months after being closed in order to evaluate re-incidence or particular patterns in the very short-term..

According to the notification the data may be ***transferred*** to involved services on a need to know basis. Within the Commission, data may be transferred to the DG ADMIN/Security, OLAF and IDOC. The report and supporting documents may also be transferred to national law enforcement agencies or judicial authorities.

Regarding the ***right to information***, the notification annexes a privacy statement intended to provide information to individuals. The privacy statement will be published on the JRC Ispra intranet website. The privacy statement is not provided directly to individuals, neither to those who act as witnesses or collaborators nor to those accused of wrongdoing.

The privacy statement contains information on identity of the data 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 time limits for storing the data and the right to have recourse at the European Data Protection Supervisor.

As far as the ***right of access and rectification***, the privacy statement declares that individuals have such rights regarding the information that SeS holds about them. It gives the name and e-mail of the contact person to exercise such rights as well as to answer any further questions regarding the processing of their personal information.

The EDPS notes that SeS has implemented ***security measures***. The security measures used to keep the report in the database ARDOS is being analysed in the context of the ARDOS prior check Opinion. Regarding the security measures applied to the paper version of the document, the Notification refers to exceptional security measures in order to limit and control access to areas where the reports and supporting documents are stored.

2.2. Legal aspects

2.2.1. Prior checking

Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter "Regulation (EC) No 45/2001") applies 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*" and to the processing "*by all*

Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part or which fall within the scope of Community law"[3].

For the reasons described below, the EDPS considers that all the elements that trigger the application of the Regulation exist in the data processing carried out by the SeS:

Firstly, in performing investigations related to accidents of different kinds *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001 are processed. 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 like SECPA and ARDOS, video surveillance footages, etc. later stored in an electronic database, personal data are processed. Finally, the EDPS confirms that the processing is carried out by a Community institution, in this case by the Joint Research Centre Ispra, which is part of the European Commission, in the framework of Community law (Article 3.1 of the Regulation (EC) No 45/2001). Therefore, clearly all the elements that trigger the application of the Regulation exist with respect to the processing operations to perform security investigations at JRC Ispra.

Assessment of whether the data processing operations fall under Article 27 of the Regulation. Article 27.1 of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS *"processing operations likely to present specific risks to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes"*. Article 27.2 of the Regulation contains a list of processing operations that are likely to present such risks. 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 SeS 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.

In addition, the EDPS considers that the notification also falls under Article 27.2(b) of the Regulation (EC) No 45/2001 which stipulates that data operations which *"evaluate personal aspects relating to the data subject, including his or her (...) conduct*" shall be subject to prior checking by the EDPS. In the case under analysis, certainly the conduct of individuals will be evaluated in order to ascertain their involvement in given occurrences, thus triggering the application of Article 27.2(b).

Ex post prior checking. Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case, however, the processing operations have already started. This is not a serious problem as far as any recommendations made by the EDPS may still be adopted accordingly.

[3] *Ex* Article 3.2 of Regulation (EC) No 45/2001.

Notification and due date for the EDPS Opinion. The notification of the DPO was received on 3 September 2007. The two-month period within which the EDPS must deliver an opinion was suspended during 299 days to obtain additional information and enable the DPO and data controller to provide comments on the EDPS Draft Opinion. The Opinion will therefore be adopted no later than 29 September 2008 (taking into account that the month of August does not count).

2.2.2. 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.

As pointed out by the Notification, of the various grounds listed under Article 5 of Regulation (EC) No 45/2001, the processing operation notified for prior checking fall 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 JRC Ispra C7 and in particular the SeS; 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 below, 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.

First, the 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. Second, the Commission Decision of 29 November 2001 also foresees a similar 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. Third, the Commission's Decision C(94) 2129 of 8 September 1994 sets forth the tasks of the Security Office. Among the ordinary tasks to be performed by the Security office, it lists the maintaining the order in Commission buildings {Article 3 (a)} as well as conducting investigations entrusted to it by the competent authority (or initiated on its own initiative when offenders are caught in *flagrante delicto*) {Article 3 (f)}. These investigations aim at ensuring secure operating conditions in the Commission or at obtaining information relating to any illegal acts occurring in its departments for the purposes of a judicial inquiry or a disciplinary action. Finally, the mission statement Security Service JRC Ispra sets forth the duties of the Security service of JRC Ispra. Among others, it is listed that the Security Service will perform investigations and enquiries regarding security related issues such as incidents, thefts, vandalism, road accidents, misuse of ICT services[4], etc.

[4] Administrative Notice 45/2006 of 15th September 2006 governing the acceptable use of the Commission's ICT Services (pc equipment, e-mail and internet access systems, telephone, fax and mobile phones) http://www.cc.cec/guide/publications/infoadm/2006/ia06045_en.html

The EDPS considers that the above legal grounds, from a more general to a more specific perspective, foresee the existence of a Commission's Security Service, with central and local offices such as that of JRC Ispra. Furthermore, the above legal grounds also foresee the kind of processing operations described in the Notification. Indeed, the legal instruments referred to above enable the Security office of the Commission the carrying out of processing operations towards obtaining information aiming at ensuring secure operating conditions in the Commission 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 is satisfied 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 JRC Ispra premises.

However, the EDPS observes that the above legal framework does not fully provide a clear crystal picture regarding the concrete tasks and competences that pertain to the Commission's security office (DG ADMIN Security Directorate) and those allocated to the security offices at the level of institutions, services and departments, such as the Security Service of JRC Ispra. In this regard, there is a question as to whether the Security Service of JRC Ispra is entitled to carry out the processing operations towards obtaining information or whether this competence is limited to the Commission's Security Office (DG ADMIN).

Given the sensitivity of the information collected, it appears necessary to have full certainty about which institution or body is entitled to carry out these activities. Therefore, the EDPS calls upon JRC Ispra in conjunction with DG ADMIN to clarify this point. If the SeS of JRC Ispra is indeed competent for the carrying out of security investigations, the EDPS calls upon JRC Ispra and DG ADMIN to consider whether it may be appropriate to enact additional legal grounds that would establish clearly the competences of the Security Service of JRC-Ispra confirming its competence, together with DG ADMIN, to perform investigations related to incidents and draft a report describing their occurrence.

Processing operations are carried out in the public interest. The EDPS notes that JRC Ispra, in particular SeS, carries out the processing activities in the legitimate exercise of its official authority. As reflected in the mission statement of the SeS, this service has the competence and the obligation to engage in investigations for the overall purpose of protecting persons, property and activities under the responsibility of JRC Ispra. 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 JRC Ispra premises it appears necessary to process personal data. Unless such data are processed it would not be possible for JRC Ispra 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 *ad hoc* incidents 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.

2.2.3. 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 2.2.2 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 JRC Ispra C7 when it engages in data processing operations, the EDPS understands that the collection of special categories of data is not JRC Ispra C7's main goal.

However, the EDPS considers that in the context of the investigation, JRC Ispra C7 may become, perhaps involuntarily, in possession of special categories of data, which will often be of no interest/relevance to the investigation. In this regard, the EDPS recalls the application of the data quality principle, 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 clearly are 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.

2.2.4. 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 will always be present in the investigation of incidents such as the name, date of birth, 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 for the principle of data quality. For example, the decision to open an investigation into an inquiry should define the subject and scope of the inquiry. This would help to reduce 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 the investigation and draft the 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 right of access, rectification, blocking and erasure (see point 2.2.7 below). Furthermore, an investigation system that guarantees the inclusion of evidence of charge and discharge is of relevance as concerns the accuracy and the completeness of the data being processed. As a consequence, and considering its importance from a data quality perspective, the EDPS recommends that security officers are made aware of this principle.

2.2.5. 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 conservation period varies depending on the categories of data. The EDPS is satisfied with the five year period that applies to information regarding cases that result in the application of effective measures (i.e. interdiction in accessing a site or a particular area). The EDPS is also satisfied with the 10 year period that applies to information that relates to cases that result in a dossier that is handled under criminal law. This deadline takes into account the period of time necessary under national legislation for crimes to be expunged.

Reports which lead to the conclusion that it was not wrongdoing or that it resulted in no effective applicable measure are kept for 12 months after being closed in order to evaluate re-incidence or particular patterns in the very short-term). The EDPS is also satisfied with this period.

2.2.6. Transfer of Data

Articles 7, 8 and 9 of Regulation (EC) No 45/2001 set forth certain obligations that apply when data 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.

Transfer of personal data within or between Community institutions or bodies. The facts described in the notifications for prior checking reveal that data are transferred to Community institutions and bodies such as OLAF, IDOC or the Security Directorate in DG ADMIN.

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 Community 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 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 extended its application to these public authorities, Article 8 of the Regulation has to be taken into account. For those countries that have not extended their implementation of Directive 95/46/EC to judicial authorities, consideration to Article 9 of the Regulation has to be given. In those cases, Council of Europe Convention 108, which for the matter under analysis can be considered as providing an adequate level of protection, is in any case applicable to judicial authorities

Since in the present context, the data are not required by the recipient, but it is JRC Ispra C7 who decides unilaterally on the transfer, JRC Ispra C7 has to establish the "necessity" of the transfer in a reasoned decision in this regard.. In order to implement this rule, as suggested above regarding data transfers to Community institutions and bodies, the EDPS recommends that JRC Ispra C7 investigators use the same approach as under Article 7 of Regulation (EC) No 45/2001 and list in a reasoned opinion all the data transfers that will be carried out or have been carried out in the context of a case and describe their necessity. These procedures should be communicated to the investigators.

2.2.7. 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 data 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 (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).

The privacy statement declares that individuals have such rights regarding the information that JRC Ispra C7 holds about them. It gives a functional email box as the contact person to exercise such rights. The practice as described in the privacy statement is in line with Article 13 of Regulation (EC) No 45/2001.

The privacy statement does not foresee the possibility, in certain cases, to defer the obligation to provide access/rectification to safeguard the investigation. However, in some instances JRC Ispra C7 may be able to rely on some of the exceptions to Article 20.1 of Regulation

(EC) No 45/2001 to defer such a right. Notably, this may be lawful where such a restriction constitutes a necessary measure to safeguard *"(a) the prevention, investigation, detection and prosecution of criminal offences;* JRC Ispra may also be able to rely on Article 20.1 (c) to defer the provision of access if it considers that deferring the information is necessary in order to safeguard *"the protection of the data subject or of the rights and freedoms of others"*, for example, if it considers that the disclosure of information may reveal the identify of the whistleblower or informant which may be the case in a number of instances. In deciding whether JRC Ispra C7 must rely on an exception, it must engage in a case-by-case assessment of the circumstances of the particular data processing at stake.

If JRC Ispra C7 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. JRC Ispra C7 must assess in each case whether the conditions for the application of one of the exceptions, for example, Article 20.1.a or 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 JRC Ispra C7 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, JRC Ispra C7 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 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 adopted on a case-by-case basis.

2.2.8. Information to the Data Subject

Pursuant to Article 11 and 12 of Regulation (EC) No 45/2001, those who collect personal data are required to inform individuals to whom the data refers of the fact that their data are being collected and processed. Individuals are further entitled to be informed of, *inter alia*, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to.

In assessing whether the data 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 in a way that enables individuals to read and store the information for further reading and, second, the extent to which the information provided, its content, 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 the Intranet of the Security Service of the Ispra site. In addition, according to the Notification, individuals, including the authors and witnesses, in cases of written and oral declarations "are *aware of the information being collected and provided*". *A fortiori*, this will not be the case when such individuals are not interviewed or do not give written declarations.

The EDPS considers that the publication on the Intranet of the Security Service of the Ispra site is a positive practice towards informing individuals. The EDPS also recognises that by

engaging in a written/oral declaration, individuals are implicitly aware of the type of data that is being collected from them. However, in the EDPS's view, the combination of these two mechanisms does not result in providing proper information to individuals in a way that they can read and store such information for future reference. In particular, the EDPS is concerned that in some instances individuals, for example witnesses, may contact the Security Service without visiting the Security Service web site, thus, bypassing the privacy statement. This is even more likely regarding the authors of the unlawful behaviour. The problem is further emphasized if one takes into account that some of the concerned individuals may not have access to the Intranet of the Security Service of the Ispra site as will be the case with external individuals. This outcome could be easily avoided if individuals were provided directly with the privacy statement. Therefore, the EDPS calls upon JRC Ispra C7 to define a procedure for providing the privacy statement to individuals about whom personal data are collected. As far as witnesses are concerned, the provision of information could be carried out in the context of accepting the verbal or written declarations. For anyone else, this could be done as a part of the procedure of the written/oral declaration that entails the signature of the declaration by the author.

In the case in point, the application of Article 20 of Regulation (EC) No 45/2001 enables JRC Ispra C7 to *defer* the provision of information to safeguard the interests mentioned in subsection (a), i.e. the prevention, investigation, detection and prosecution of criminal offences. JRC Ispra C7 may also rely on section (c) if it considers that deferring the information is necessary in order to safeguard *"the protection of the data subject or of the rights and freedoms of others",* for example, if it considers that the disclosure of information may reveal the identify of the whistleblower or informant which may be the case in a number of instances. In deciding whether JRC Ispra C7 is under the obligation to provide information or whether an exception applies, JRC Ispra C7 must engage in a case-by-case assessment of the circumstances of the particular data processing at stake.

If JRC Ispra C7 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. It must assess in each case whether the conditions for the application of one of the exceptions, for example, Article 20.1.a or 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. Finally, if JRC Ispra C7 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, JRC Ispra C7 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."*

The content of the privacy statement.- The EDPS has also checked the content of the information provided in the privacy 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 data 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 privacy statement lacks the following information and calls upon JRC Ispra C7 to complete it.

Firstly, the EDPS considers that the privacy statement should refer to the legal basis enabling JRC Ispra C7 to carry out the data processing. This is particularly important if one takes into account the rather sensitive type of data processing which may result in a person being brought before the criminal justice. Secondly, the EDPS considers that the description of the purposes of the processing is not complete as it fails to describe the intended final use of the report carried out by JRC Ispra C7. Finally the EDPS 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.

2.2.9. 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. JRC confirms that it adopted the security measures required under Article 22 of the Regulation. The EDPS has no reason to believe that JRC 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.

3. 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, JRC Ispra C7 must be aware of the following:

- There is a need for JRC Ispra, together with DG ADMIN, to clarify the competences of the Security Service of JRC Ispra, particularly to confirm their competence, together with DG ADMIN, to perform investigations related to incidents and draft a report describing their occurrence.
- 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 rule.
- When data are transferred within EU institutions and bodies and also to national (police and judicial) authorities 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.
- When possible, the privacy statement should be provided directly to data subjects. A procedure to this effect should be set up.
- The privacy statement should be amended as suggested in this Opinion.

Done at Brussels, 31 July 2008

(signed)

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor