Opinion on a notification for prior checking received from the Data Protection Officer of the General Secretariat of the Council of the European Union (GSC) on the conduct of investigations by the Security Office

Brussels, 12 December 2008 (Case 2008-0410)

1. Procedure

On 2 July 2008, the European Data Protection Supervisor (EDPS) received from the Data Protection Officer (DPO) of the GSC a notification for prior checking on the conduct of investigations by the GSC's Security Office.

On 25 July the EDPS asked the controller to provide additional information. The answers were received on 12 August 2008. The controller was sent a further list of questions on 17 September 2008, which were answered on 15 October 2008. The draft opinion was sent for comment to the DPO on 30 October 2008. The EDPS received the DPO's comments on 8 December 2008.

2. The facts

The ***purpose*** of GSC Security Office investigations is to investigate and prosecute criminal offences and to investigate and report breaches of the Council's security regulations [1], whether committed by negligence or with the intention of compromising classified information. Secondly, the investigations serve to prevent the various breaches and acts of negligence, disclosure and compromise mentioned above. GSC Security Office investigations/enquiries also comprise counter-intelligence investigations.

The notification referred solely to investigations conducted by the GSC Security Office and did not cover the Security Office's related activities; the latter are therefore not dealt with by the EDPS in this opinion.

The procedure involves recording all investigations made by the EU Classified Information (EUCI) Security/Investigation Sector of the Security Office. This means that a record is kept of every security incident and operation, every item of intelligence and every case of assistance provided to the Belgian or other authorities. These records make it possible to study incidents over the short and long term and to analyse the threats and risks that they entail. They are also essential to the Appointing Authority when issuing the authorisations (security clearance and authorisation for staff to access information) referred to in paragraphs 4 and 5 of Part II.VI of Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations. Paragraph 5 lays down that authorisation shall be withdrawn by the appointing authority where it considers there are justifiable grounds for doing so. Any decision to withdraw authorisation shall be notified to the person concerned, who may ask to be heard by the appointing authority, and to the competent national authority.

[1] Council Decision of 19 March 2001 adopting the Council's security regulations (2001/264/EC)

Anyone concerned by an investigation conducted by the GSC Security Office is a data subject of the processing operation under consideration. The groups of persons concerned include the following: officials and other staff in active employment at the GSC; retired officials and other staff, service providers, seconded national experts, interns, Member States' delegates, officials of other Community institutions, visitors, journalists, Member States' civil servants, staff of outside firms, and the family members of the persons in the aforementioned groups.

Which ***data*** are processed will depend on the facts ascertained during the investigations. They may be administrative and may also be judicial.

Each investigation is specific and requires its own categories of data, for example: badge reader recordings, data on the use of TESA/KABA cards, analysis of modus operandi (the pattern of a repeated malicious action), photographs, information on suspect vehicles, records of video-surveillance cameras and of the traffic data of telephone and electronic communications.

Some databases are automatically linked to the "Conduct of investigations" database. This is true for the database for journalists' accreditation [2], the security clearance database and the Security Centre's electronic logbook (operates 24/7). Thus the processed data also come from these databases.

In principle processing is ***automated***. Classified documents (within the meaning of Decision 2001/264/EC adopting the Council's security regulations) or sensitive files, however, are processed and stored in paper form (***manual procedure***) or on a stand-alone computer.

The Security Office directs all the investigations provided for in Decision 198/03 of the Secretary-General of the Council/High Representative concerning the tasks of the Security Office. An investigation draws together all the information collected and all the steps taken to solve problems arising from one or more security incidents. The record of that information and that action is kept in the form of automated documents, which are produced from data imported from various databases with the addition of other data. An investigation comprises four stages as follows: launch of the investigation; initial investigation; further investigations; the report on the investigation and the analysis of the findings.

(a) An investigation may be launched under a wide variety of circumstances, with incident reports being the most frequent trigger. An incident report is an electronic form to be found on the Security Office's website and is available to everyone with access to the GSC's intranet. Other important triggers are as follows: being caught in the act (the investigation is then opened at the investigator's behest); an entry in the Security Centre's logbook, which records all incidents 24/7; reports by the GSC's security guard service; an official request from the authorities of Belgium or another Member State; an official request from another institution's investigation department, and a request from the appointing authority.

[2] The EDPS has considered the processing of data on the accreditation of journalists (Case 2004-0259); see opinion published on 16 September 2008.

(b) the initial investigation aims to gather all the information at the scene of the incident: eyewitness accounts; identification of all persons present at the scene; preservation of evidence; interviewing victims; questioning perpetrators, and relevant photographs. At this initial investigation stage, the coordination with other departments concerned is also established.

(c) During its further investigations the Security Office will collect relevant information, interview witnesses and suspects (within the strict framework of Article 6 of Decision 198/03), where necessary inform and assist the Belgian or other police forces, seek the assistance of DGA 5 (Information and Communication Systems), and carry out searches and checks using the Security Office database. All means of collecting information are used: recordings by video-surveillance equipment and access badge readers, traffic data of service telephone communications, and electronic traffic data. The Security Office will also make use of all relevant outside and in-house contacts when conducting its enquiries.

(d) In the last stage the facts are analysed: There is a specific "conduct of investigations" application for consulting and updating the data collected. The fact that the information is stored in a dedicated database makes for more efficient long-term analysis. To record each stage of the investigations it is necessary to log into the database. The database is able to produce a report in Word.

Investigation files (both paper and electronic) are kept by the EUCI Security/Investigation Sector for a period of 30 years. The GSC gives the following reasons for this ***retention period***: (i) in Belgium serious crimes are time-barred after 20 years, and the EUCI Security/Investigation Sector must be able to answer questions from Belgian or other authorities on acts committed several years earlier. (ii) Some intelligence, espionage or terrorist cases may drag on for very long periods (this may be decades); (iii) the average length of an official's career is around 30 years; information on the different stages of that career and incidents during it is essential for establishing the profile of someone involved in complex investigations.

The ***recipients*** of the data: these are within the GSC (the appointing authority, the disciplinary board in the case of an ongoing administrative enquiry, and DGA 1 in the case of dealings with the GSC's insurer (e.g. sending the name of the witness of an accident)), within other Community institutions (e.g. OLAF), or outside the Community institutions, which is the case with data sent to the judicial authorities of the Member States). The data are transferred as a Word format report, with the raw data on which the report is based staying at the Security Office.

Data subjects' rights are protected under Section 5 of the Council Decision of 13 September 2004 adopting implementing rules concerning Regulation (EC) No 45/2001 of the European Parliament and of the Council 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, which sets out the procedure for data subjects to exercise their rights.

Data subjects are supplied with the requisite information via Decision 198/03 of the Secretary-General of the Council/High Representative concerning the tasks of the Security Office, of which all staff are apprised. More specifically Article 6(3) of the Decision states: "where the possible personal implication of an official or servant of the General Secretariat emerges, the interested party shall be informed rapidly by the Security Office. The provision of this information can be deferred with the agreement of the Deputy Secretary-General if it would jeopardise the investigation, or in cases necessitating the maintenance of absolute secrecy for the purposes of the investigation and requiring the use of investigative procedures falling within the remit of a national judicial authority. In any event, conclusions referring by name to any such person may not be drawn once the investigation has been completed without the interested party having been enabled to express his views on all the facts that concern him."

The different categories of data can be ***blocked*** and ***erased*** within two working days on the basis of a legitimate request from the data subject.

The ***security measures*** in place require data to be stored in special electronic files created by a dedicated database, the Ibase, (a sophisticated dedicated intelligence database for collecting, checking and analysing data from multiple sources in a secure environment) and to be kept on the server reserved for security applications, access to which is restricted to the investigators directly handling the investigations and their head of unit. Investigators have access to all files because of the potential links between investigations. It should be noted that the investigators are few in number (three or four). The server and the interconnected and stand-alone work stations can only be accessed using a special A75 USB stick.

Access to the application itself requires user name identification and is password protected. Investigation files that are sensitive or classified CONFIDENTIEL UE and above are placed in a secure cupboard and kept in the EUCI Investigation/Security Sector's offices, which are themselves protected with security locks which record every entry. All investigators have received security clearance up to SECRET UE or above.

3. Legal aspects

3.1. Prior checking

This prior checking relates to the processing of personal data ("*any information relating to an identified or identifiable natural person*", Article 2(a) of Regulation (EC) No 45/2001 (hereinafter "the Regulation") in connection with security investigations conducted by the GSC Security Office. Processing consists of the collection, consultation, storage, erasure, etc. of data. It is carried out by a European institution in the exercise of activities part of which fall within the scope of Community law. The processing of personal data is largely by automatic means. As a consequence, the Regulation is applicable.

Article 27(1) of the Regulation makes all "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*" subject to prior checking by the EDPS. Article 27(2)of the Regulation lists the processing operations likely to present such risks.

Article 27(2)(b) of the Regulation stipulates that processing operations intended to "*evaluate personal aspects relating to the data subject, including his or her (...) conduct*" are subject to prior checking by the EDPS. In the case considered here, the Security Office examines officials' conduct.

Under Article 27(2)(a) of the Regulation, processing of data relating to "*suspected offences, offences, criminal convictions or security measures*" are also subject to prior checking by the EDPS. In the case under consideration, this type of data is also processed.

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 operation has already started. This should not be a serious problem, as the recommendations of the EDPS may still be adopted accordingly.

The notification of the DPO was received on 2 July 2008. In accordance with Article 27(4), this opinion must be delivered within a period of two months of that date. The procedure was suspended for a period of 102 days (71 days' suspension + the month of August). The opinion is therefore to be adopted no later than 15 December 2008.

3.2. Legal basis and lawfulness of the processing operation

The processing of data in connection with security investigations is based on various legal instruments, which range from the very general to the very specific. The Council's Rules of Procedure (Decision 2006/683/EC) stipulate that: *"The Council shall decide on the organisation of the General Secretariat. Under its authority the Secretary-General and the Deputy Secretary-General shall take all the measures necessary to ensure the smooth running of the General Secretariat"* (Article 23).

The Council's security regulations adopted by Decision 2001/264/EC provide a legal basis for establishing a comprehensive security system for the Council, the General Secretariat and the Member States with regard to their activities in areas requiring a degree of confidentiality. Section I of Part II of the regulations gives the Secretary-General/High Representative responsibility for investigating or ordering an investigation into any leakage of EU classified information which, on prima facie evidence, has occurred in the GSC or any of the EU decentralised agencies. Section I also establishes the Security Office, tasked with coordinating, supervising and implementing security measures. Section X covers the definition of breaches of security and the compromise of EU classified information and how these are dealt with. It also describes in detail the security authority's role should a security breach occur or EU classified information be compromised.

Lastly, Decision 198/03 of the Secretary-General/High Representative describes in even greater detail the remit of the Security Office and more specifically its investigations.

Article 2 states: *"[t]o this end, the Security Office shall, in conformity with the Security Regulations: (…) investigate any leakage, unauthorised disclosure or compromise of EU classified information which, on prima facie evidence, has occurred in the General Secretariat or any of the EU decentralised agencies."*

Article 5 provides: *"Where a person is caught in the act of committing any act or omission contrary to the criminal law of the host State, the Security Office shall carry out an immediate enquiry and may detain, in conformity with the law of the host State, the person concerned until the competent national authorities have been contacted and are in a position to question him."*

Article 6 states: *"Without prejudice to its obligation to assist the European Anti Fraud Office in the practical conduct of its investigations, whenever the Security Office suspects or has information indicating that, an offence has been committed, is in the process of being committed or is likely to be committed within a Council building or place of work, it shall inform the Secretary-General/High Representative or the Deputy Secretary-General immediately thereof and conduct an enquiry. When conducting enquiries, the Security Office may, with the authorisation of the Secretary-General/High Representative or of the Deputy Secretary-General and in cases of extreme urgency:*

- *interview any person present within a Council building or place of work;*
- *have access to any premises within the Council buildings or place of work;*
- *have access to all documents and information to the extent necessary for the enquiry.*

2. Information forwarded or obtained in the course of internal investigations, in whatever form, shall be subject to professional secrecy and shall enjoy the protection given by Regulation (EC) No 45/2001 and/or other provisions applicable to the Council.
Under Article 11: *Investigations of security related matters are the responsibility of the Security Office under the direction of the Secretary General/High Representative or of the Deputy Secretary-General. No staff member or contracted third party of the General Secretariat may conduct investigations into security related matters without prior approval of the Secretary-General/High Representative or of the Deputy Secretary-General."*

Article 15 states that: *"The Security Office may establish contact with:*
the competent National Security Authorities of Member States to elicit their assistance with regard to the information it needs to assess such dangers and threats as may face the General Secretariat, its staff, its activities, its assets and resources and its classified information at its usual place of business;
the competent national services of the Member States or Host States on the territory of which the General Secretariat may exercise its activity, regarding any matter relating to the protection of its staff, its activity, its assets and resources, and its classified information while on their territory;
the security services of the other European institutions and international bodies, with a view to any useful coordination."

The lawfulness of the processing operation must be considered in the light of this legal basis. Article 5(a) of the Regulation stipulates that personal data may be processed only if: "*processing is necessary for the 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 or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed*". As the instruments referred to above demonstrate, the investigations conducted by the Security Office are tasks carried out in the public interest (dealing with and preventing security breaches, the compromise of EU classified information, etc.) on the basis of legal instruments adopted on the basis of the Treaties. Furthermore, the Security Office carries out those activities in the legitimate exercise of official authority and thus is complying with its legal obligation to investigate matters within its remit.

Whether or not the processing operation is "necessary" has to be considered in terms of specifics. From this perspective, it should be borne in mind that the processing of personal data as part of investigations has to be proportional to the overall purpose of the processing operation (i.e. investigating criminal offences, protecting people, property, information, etc.) and to the specific purpose of the processing operation in the context of the case under investigation. For instance, the seriousness of the incident under investigation has to be considered, as does the type of data needed to clarify the facts, etc. This also means that other, less intrusive methods, if any, should be found. The question of the proportionality of processing has therefore to be evaluated on a case-by-case basis. Subject to such case-by-case examination, the proposed processing operation is lawful.

3.3. Processing of special categories of data

Article 10(5) of the Regulation stipulates as follows: *"Processing 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 case under consideration, the processing of the data concerned is authorised by the legal instruments mentioned above in section 3.2.

Under Article 10(1) of the Regulation, the processing of special categories of data (i.e. "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and (...) data concerning health or sex life*") is prohibited. Article 10(2) of the Regulation provides for certain exceptions. The exception, if any, which would very probably apply would be that under Article 10(2)(d) ("*processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims"*).

The type of data described in Article 10(1) will not be processed routinely but may certainly play a role in some investigations. In that case, the blanket prohibition on processing such data set out in Article 10(1) should be followed, or otherwise there should be strict examination of the need for an exception to be applied.
In either case, Security Office staff dealing with such cases must bear in mind that these are exceptions and that special categories of data are to be excluded unless a case is characterised by one of the circumstances listed in Article 10(2) or it is necessary to apply Article 10(4) of the Regulation. *("Subject to the provision of appropriate safeguards, and for reasons of substantial public interest, exemptions in addition to those laid down in paragraph 2 may be laid down by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by decision of the European Data Protection Supervisor*").

3.4. Data quality

Under Article 4(1)(c), personal data must be "*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.*"

Even though certain standard data (name, category of person, etc.) will be routinely included in investigation files, the precise content of a file will of course vary according to the case. The quality of the data has therefore to be assessed case by case. Safeguards should be provided to ensure compliance with the principle of data quality. These could take the form of a general recommendation to staff handling such files, reminding them of the rule and asking them to make sure that it is complied with.

Article 4(1)(d) of the Regulation requires that personal data be "*accurate and, where necessary, kept up to date*", and specifies that "*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*". It is reasonable to believe that, given the procedure established (dedicated investigation database in which data can be updated), the data are accurate and kept up to date. This principle (of accurate data kept up to date) is closely linked to the exercise of the right of access, rectification, blocking and erasure (see section 3.7 below).

Data must also be "*processed fairly and lawfully*" (Article 4(1)(a) of the Regulation). The question of lawfulness has already been considered. That of fairness warrants close attention in view of the sensitivity of matter in hand. It arises in connection with the information given to the person subject to investigation (and other to data subjects, whether witnesses, informants, or other), and the speed with which that information is provided, in order that the right of defence can be respected (see section 3.8 below).

3.5. Data storage

Personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The Community institution or body shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes*" (Article 4(1)(e) of the Regulation).

Data kept in the electronic database and physical files are stored for thirty years from the time a case is opened. As noted earlier, the Security Office gives three reasons for setting this data storage period. Firstly, under Belgian law the time bar for prosecuting serious crimes is generally 20 years; the officials who have dealt with such cases may be required to give evidence before the competent bodies. Secondly, some intelligence and counter-espionage cases can only be assessed over the long or the very long term; thirdly, an official's career lasts 30 years on average.

In addition, under Article 37(1), traffic data, i.e. is the data necessary to establish calls, are deleted or made anonymous once calls are finished. Article 20 provides for exceptions to this rule, in particular where such exemptions are necessary "to safeguard the protection of the data subject" or "the national security, public security or defence of the Member States".

The EDPS considers that this data storage policy complies with the provisions of the Regulation.

3.6. Data transfer

3.6.1. Transfer of personal data within or between Community institutions or bodies

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.*"
This means that the reports and/or the related documents (personal data) will be transferred only if this is "necessary" for the legitimate performance of tasks covered by the competence of the recipient. 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. Under Article 7(2), where the data are transferred following a request from the recipient, both the controller and the recipient bear the responsibility for the legitimacy of the transfer. It is incumbent on the Security Office to verify the competence of the recipient and to make a provisional assessment of the necessity for the transfer of the data. If doubts arise as to this necessity, the Security Office must seek further information from the recipient.

In any event, under Article 7(3) of the Regulation the recipient must be informed that personal data may be processed only for the purposes for which they were transmitted.

In addition, the Security Office should add a note to the file to the effect that the data have been transferred.

3.6.2. Transfer of personal data to Member States
Member States fall into two categories with regard to such transfer:

(a) Member States whose national data protection law adopted pursuant to Directive 95/46/EC [on the protection of individuals with regard to the processing of personal data and on the free movement of such data] covers every sector of the national legal system, including the judicial sector;

(b) Member States whose national data protection law adopted pursuant to Directive 95/46/EC does not cover every sector, and, in particular, does not cover the judicial sector.

As far as the situation in the first group is concerned, Article 8 of the Regulation provides that: *"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, or (…)".*

Thus, even if judicial authorities do not fall within the scope of Directive 95/46/EC, Article 8 of the Regulation has to be taken into account if the Member State extended application of the Directive to those public authorities when incorporating the Directive into national law.

Although, under Article 8(a) of the Regulation, it is for the recipient to establish the interest and need to receive the data, the EDPS considers that, in view of the Security Office's specific activities, this provision should be construed as meaning that if the information is not being sent at the recipient's request, it is the sender's task to verify that the transfer is necessary. Thus, where the Security Office sends personal data to competent national authorities on its own initiative, it should establish that those data are necessary for the performance of a task carried out in the public interest. The Security Office must make such an assessment whenever it transfers personal data on its own initiative and should draw up a reasoned decision demonstrating that the transfer is necessary.

In order to comply with Article 8(a) of the Regulation, the recipients of the data must use them to perform a task in the public interest. The EDPS considers that the transfer of personal data in mutual assistance exchanges may in abstract be regarded as fulfilling the requirement of Article 8(a). The data will be used by Member States' competent authorities to perform tasks in the public interest, i.e. intelligence activities.

For countries in which Directive 95/46/EC does not cover the judicial authorities, Article 9 of the Regulation must be taken into account. In those countries, Council of Europe Convention 108, which on this question may be considered to provide an adequate level of protection, is in any case applicable to judicial authorities.

3.6.3. Transfer to third-country authorities and/or international organisations
Article 9(1) of the Regulation 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 States which do not provide an adequate level of protection.

However, Article 9(6) provides for exceptions, in particular if "*the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims*" (Article 9(6)(d)). Since this is an exception, it must be interpreted strictly; it must not be used systematically. Only occasional application of the derogation is admissible, in cases where the purpose of the processing operation makes it particularly necessary to transfer the data. In any event, recourse to Article 9(6) must not lead to the infringement of the data subject's fundamental rights.

Article 9(7) provides for another kind of exception; it stipulates that the EDPS may authorise the transfer of personal data "*where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights*; *such safeguards may in particular result from appropriate contractual clauses*".

Under Article 9(8), the Security Office must inform the EDPS of categories of cases where it has applied Article 9(6) and (7). The EDPS accordingly recommends introducing a register of occasional transfers made pursuant to the derogations set out in Article 9(6) and (7). The register could include the following information: purpose of the transfer, data subjects, categories of data, information provided to the data subjects (if applicable), rights of access (direct or indirect), legal basis and lawfulness of the transfer, recipients of the data, how long the recipient will store the data, and so on. The EDPS should be available for consultation by the EDPS at all times.

The EDPS is aware that Section XII of Decision 2001/264/EC sets out the principles regulating the release of EU classified information to third states or international organisations. Article 3 of Section XII provides that: "*the acceptance of EU classified information by third States or international organisations will imply an assurance that the information will be used for no purposes other than those motivating the release or exchange of information, and that they will provide the protection required by the Council"*. The EDPS has highlighted this point, commending the fact that such transfers are subject to the strict security requirements laid down in Decision 2001/264/EC; he would stress, however, that such transfers must also - as explained earlier - meet the data protection requirements under Regulation No 45/2001.

3.7. Right of access and rectification

Under Article 13 of the Regulation, the data subject has the right to obtain, without constraint, from the controller, communication in an intelligible form of the data undergoing processing and of any available information as to their source.

The right of access is the data subject's right to be informed of any information relating to him or her that is processed by the controller. As a matter of principle, that right has to be interpreted in conjunction with the concept of personal data. The Regulation adopts a broad concept of personal data, and the Article 29 Working Party's interpretation of the concept has been similarly broad [3]. There is a direct link between respect for the rights of access and rectification and the principle of data quality and, in the context of investigations, that respect overlaps to a great extent with the right of defence.

The right of access is also applicable when a data subject requests access to the files of others, where these contain information relating to him or her. This would be the case of informants or witnesses who demand access to the data relating to them included in an investigation conducted on another person.

The information can be obtained directly by the data subject ("direct access") or, in certain circumstances, by a public authority ("indirect access", normally exercised by a Data Protection Authority, in the present context by the EDPS).

As mentioned in section 2 above, the Council adopted the Decision of 13 September 2004 adopting implementing rules concerning Regulation (EC) No 45/2001 of the European Parliament and of the Council 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, Section 5 of which sets out the procedure for data subjects to exercise their rights.

The EDPS welcomes the fact that the data subject's rights of access and rectification are guaranteed. He recognises that those two rights may be restricted in accordance with Article 20 of the Regulation in certain circumstances (see below). Those restrictions must be "necessary". This means that the "necessity test" should be conducted on a case-by-case basis, and that the rights of access and rectification, like the right of information, will have to be safeguarded, provided that this does not risk compromising the investigation (see section 3.8 below).

The restrictions specified in Article 20 of the Regulation concern in particular cases where such restriction constitutes a necessary measure to safeguard "*(a) the prevention, investigation, detection and prosecution of criminal offences*; *(b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters; (c) the protection of the data subject or of the rights and freedoms of others"*. Moreover, in certain cases it may be necessary to deny the data subject direct access so as not to hinder the proper conduct of the investigation even though this is a "pre-disciplinary" or "pre-criminal" inquiry rather than a criminal investigation within the meaning of Article 20 of the Regulation. The interests of the authority tasked with following the investigation (OLAF, national authorities) may also be taken into account here.

[3] Cf. Opinion 4/2007 on the concept of personal data adopted by the Article 29 Data Protection Working Party (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf).

In any event, the Security Office must take into account and comply with Article 20(3): *"If a restriction provided by paragraph 1 is imposed, 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."* Concerning the right to information, this provision has to be read in conjunction with Articles 11, 12 and 20 of the Regulation (see section 3.8 below).

Moreover, account should also be taken of Article 20(4): *"If a restriction provided for by paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made."* The right of indirect access will then have to be ensured. This provision will be relevant, for instance, in cases where the data subject has been informed or is aware of the processing operation but has restricted right of access in the light of Article 20.

Article 20(5) states that "*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*." It may be necessary for the Security Office to postpone providing such information in accordance with this provision, in order to safeguard the investigation. Whether or not such a deferral is necessary must be determined on a case-by-case basis.

As already mentioned, the right of access entails the data subject's right to be informed about the data referring to him or her. However, as noted above, that right may be restricted to safeguard "*the protection of the (...) rights and freedoms of others*", a restriction which needs to be taken into account in the case under examination when considering the data subject's access to the identity of whistleblowers. The Article 29 Working Party has states as follows: *"[u]nder no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblower (…) on the basis of the accused person's right of access, except where the whistleblower maliciously makes a false statement. Otherwise, the whistleblower's confidentiality should always be guaranteed*." The same approach should be applied to informants[4].

Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data. Given the sensitivity of most investigations conducted by the Security Office, this right is crucial in guaranteeing the quality of the data used, which is linked in this case to the right of defence. The right to rectification also requires that the rectification of inaccurate or incomplete data be notified to third parties to whom the data have been disclosed, as laid down in Article 17. Any restriction under Article 20 of the Regulation must be applied in the light of what has been said in the preceding paragraphs regarding the right of access.

Finally, rules must be established so that once an investigation is closed, the official under investigation can rectify any data concerning him or her by requesting that documentation relating to any subsequent developments during the follow-up phase should be added to the investigation file.

[4] The identity of witnesses, however, does not have to remain confidential.

3.8. Information supplied to the data subject

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

Article 11 of the Regulation (*Information to be supplied where the data have been obtained from the data subject*) and Article 12 (*Information to be supplied where the data have not been obtained from the data subject*) are therefore both applicable to the present case. This means that the relevant information must be given either at the time of collection (Article 11) or when the data are first recorded or disclosed to a third party (Article 12) unless the data subject already has that information.

As noted in section 2, in a case involving a member of the GSC staff, he or she will be rapidly informed by the Security Office unless this would jeopardise the investigation, or in cases necessitating the maintenance of absolute secrecy for the purposes of the investigation and requiring the use of investigative procedures falling within the remit of a national judicial authority. "*In any event, conclusions referring by name to any such person may not be drawn once the investigation has been completed without the interested party having been enabled to express his views on all the facts that concern him*." (Article 6(3) of Decision 198/03). Decision 198/03 may be consulted on the GSC's intranet.

The EDPS welcomes the fact that the information is provided in two ways: generally, in the form of the published decision and individually, when the Security Office personally informs the data subject.

However, the EDPS finds that, even if in content the information provided may at times partially match the mandatory information under Articles 11 and 12, not all the information referred to in those Articles is in fact supplied. It should be borne in mind that all the requirements under Article 11(1) and Article 12(1) must be complied with, including those under subparagraph (f): given the sensitivity of the cases in question, data subjects must be informed of all the safeguards on which they may rely. Provision of a specific privacy statement would be welcome.

As to the timing, where intelligence activities are conducted as part of an investigation, the information has to be given at an appropriate time, i.e. when it will not harm the investigation. The point at which the information is provided may not be that when the data are first recorded or disclosed, bearing in mind Article 20 of the Regulation (see below).

In cases where the Security Office does not take the written statement or have any contact with the data subject before transferring the data to a third party (OLAF, national authorities), it must, in accordance with Article 12 of the Regulation, inform the data subject as soon as the data relating to him is recorded or no later that the moment when the data are first disclosed to the third party. This recommendation obviously does not concern situations where contact with the data subject is impossible for practical reasons (where the person has disappeared or is on the run, etc.).

As already noted, Article 20 of the Regulation provides for certain restrictions on the right of information (see section 3.8. above).

Furthermore, Article 20(5) of the Regulation will have to be applied in specific circumstances: *"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 provides for 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 recourse to the EDPS; paragraph 4 provides for the indirect right of access via the EDPS and for the results of such access to be provided to the data subject; paragraph 4 provides for the indirect right of access via the EDPS and for the results of such access to be provided to the data subject).

3.9. Security measures

Some security measures have been taken. The conditions for data protection and physical access are those required by the Council Decision of 19 March 2001 adopting the Council's security regulations (2001/264/EC). Generally speaking, physical and computer access is restricted to staff with the need to know and with the appropriate security clearance/authorisation for access to classified information.

The EDPS considers that the full set of security measures taken can be regarded as adequate within the meaning of Article 22 of the Regulation.

Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation (EC) No 45/2001 provided that the considerations in this opinion are fully taken into account. In particular, the GSC should:

- evaluate the proportionality of the processing activities on a case-by-case basis;
- draw up a general recommendation to persons handling investigation files reminding them of the principle of data quality and recommending that they ensure it is complied with;
- introduce, in accordance with Article 7(1) of the Regulation, a notice to the recipient informing him/her that personal data may be processed only for the purposes for which they were transmitted;
- in cases where the Security Office is to transfer data at the recipient's request, verify the competence of the recipient and make a provisional evaluation of the need to transfer data in accordance with Article 7(2);
- add a note to the investigation file recording that the data has been transferred.
- provide a reasoned decision to demonstrate the necessity of own-initiative transfers of data to judicial authorities, in the light of Article 8 of the Regulation;
- introduce a register of occasional transfers made pursuant to the derogation under Article 9(6) and (7) and notify the EDPS thereof;
- inform the data subject as soon as his data are recorded or no later that the first disclosure of those data to third parties (Article 12);
- whenever a restriction based on Article 20 of the Regulation is applied, record it in the file;
- inform the data subject in accordance with Article 20(3) and (4) of the Regulation, where applicable;

- establish rules to ensure that once the investigation is closed the data subject can rectify his personal data and have them updated in the light of subsequent developments;
- respect the content of the information to be given to the data subject, as specified in Article 11(1) and Article 12(1) of the Regulation (including subparagraph f).

Done at Brussels, 12 December 2008.

(**signed**)

Peter HUSTINX
European Data Protection Supervisor