

Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the processing of personal data in DG ENTR Enterprise Data Warehouse.

Brussels, 19 May 2009 (Case 2008-487)

1. Proceedings

On 22 August 2008, the European Data Protection Supervisor (EDPS) received from the Data Protection Officer (DPO) of the European Commission a notification for prior checking relating to the processing of personal data in DG ENTR "Entreprise Data Warehouse".

A draft Privacy statement and a file with the different data fields were attached to the notification.

The case was suspended while further information was sought on 6 October 2008 and an answer was provided on 28 November 2008. The case was suspended again pending comments on facts of the case on 3 December 2008. After a partial reply, it was agreed to hold a meeting between staff of the EDPS and the data controller. This meeting took place on 1st April 2009 and further documents to complement the case were provided on 21 April. The case was suspended again pending comments on the draft opinion from the DPO on 4 May 2009 and these were provided on 19 May 2009.

2. Examination of the matter

The DG ENTR Data Warehouse (EDW) is a system in charge of retrieving data from multiple data sources (ABAC, COMREF, SYSLOG and DG ENTR's in-house financial data) in order to process and cross them between each other in view of obtaining measurements (metrics), indicators and reports on the activities of the DG (e.g.: by crossing financial data with HR data.). EDW is aimed at retrieving data coming from different domains, and make them interact. Based on the compiled information, DG ENTR will create reports. It is underlined that the reports that shall be created on EDW are solely for DG ENTR's internal purpose.

The main goal is to provide managers with powerful reports presenting metrics of performance, like the 'Scoreboard' report, at destination of the Head of Units, Directors and Director General. This report is made of a set of metrics presenting the "health" of the DG at several stages: Financial, HR, acquis communautaire etc.

The EDW retrieves data from the following institutional databases of other DGs of the European Commission:

- COMREF (ADMIN's database exposing SYSPER2 data to the DGs)
- SYSLOG

- DWU (ABAC data warehouse of DG BUDG)

In addition to the institutional data from other DGs, specific information from DG ENTR databases is also inserted in the system:

- Data coming from PLATO: ENTR system supporting the Activity Based Management
- Data coming from XLS file managed by Public Procurement & Grant Management Team
- Data coming from MICE: ENTR system supporting project management activities
- Data coming from CICERO: "Circuit & role" management.

The processing is articulated in 3 steps named 'E-T-L':

- The first step is aimed at extracting data from data sources.
- The second step is aimed at implementing the gateways between data (example: the column 'username' in ABAC must match an employee in SYSPER2), performing the calculation (calculating the metrics) and implementing the rejection rules (for data quality sake).
- The third step is simply aimed at loading the new data in production area (with backup procedures, in case the loading turned bad).

According to the notification, senior management at DG ENTR expressed the need to generate data that reflect how ENTR projects progress in the DG. These data should be presented under the form of a management scoreboard bringing together data from different sources considered as containing relevant status information¹.

The notification also specifies that automation will make the scoreboard more reliable from the data quality point of view; that it will free up human resources, occupied now by collecting and verifying the data, resulting in the possibility to increase the generation frequency and even to provide real-time generation leading to more effective control and steering. The automation will also offer drill down capabilities which will allow Top Management to get into details (drill down at unit, directorate level, budget line, AMP actions and staff members level) in their day-to-day analysis.

According to the notification, the EDW is then aimed at ensuring an efficient management through:

- providing management metrics: senior and middle management must be able to measure performance (via performance indicators) and use the conclusions for steering the entities they are responsible for (whether this is at unit, directorate or DG level). As an example, ENTR's Director General must have at his disposal a scoreboard report presenting major metrics like: ratio of payment execution, payment delays, total number of vacant jobs, average number of training days per employee, average number of absence days per employee.
- improving data quality and data crossing capabilities between institutional data. The managers and front line employees are drowning in data and then cannot use them efficiently. Moreover, most of the data are isolated on a temporary base because they belong to different business domains, hosted on different databases (eg: DWI Webi, SYSPER2 Webi, Sylsog Webi). Crossing these data means manual operations to be performed by front line employees. It results in an expensive and unrewarding recurrent burden of work, leading to poor data quality and hence, unreliable reports.

¹ Today, the management scoreboard is subdivided into three parts: financial resources, human resources, and other operational information like internal audit actions and questions of the European Parliament.

- providing data crossing capabilities between institutional data and ENTR data².

According to the data controller, the need for an automatic scoreboard explains the initial reason of the EDW project. But EDW is not only aimed at supplying management metrics; when a management metric is abnormal³, an investigation must be realised in order to explain the reason. Drill down to more detailed data must be achieved, sometimes at the lowest level, but with restricted access.

Also, according to the notification, with the use of the system, the initial purpose of the individual source data warehouses or data providers of the processing is not supposed to be changed but it is mainly to resolve some technical limitations which prevent answering some fundamental business requirements:

- Impossibility to create reports with the reporting tool "Business Objects" which would compile data from different databases hosted on different physical servers. EDW is aimed at being the single data repository, where the data would be hosted on the same physical server;
- Institutional databases are not communicating between each other. For instance, at the beginning SYSPER2 data warehouse could not exchange data with ABAC data warehouse, and gateways between SYSLOG data warehouse and SYSPER2 were really limited. These limitations prevented from processing metrics like the one on the obligatory trainings to be followed by ABAC users.

In the future, and in the context of the IT Governance supported by DIGIT, EDW might be deployed at EC level, and reports created on EDW shall be solely for EC's internal purpose.

It is finally explained that DIGIT recognises the need for Data warehousing. As such there are already the data warehouses on specific domains and the next step will be a institutional data warehouse combining them. DG ENTR submitted a vision document on this project which was approved by DIGIT's Corporate Protect Officer on 7/11/2006 (reference: DIGIT B/2 D(2006) 5888)

Legal basis

According to the notification, the processing operation of this Directorate General (DG) internal system is necessary for the performance and the support of the numerous tasks carried out by the DG in the interest of the institution as mandated by the Treaties, and more specifically articles 6, 7, 211, 219 and 255 of the Treaty of Amsterdam.

DG ENTR considers as additional legal basis the following notes and communications issued by DG ADMIN, DG BUDG, SG:

- ABM Communications SEC(2001) 1197/6&7 and COM(2003) 28;
- AAR Communication SEC(2001) 875/6 (Ref. action 82 of White paper);
- APB, APS and CLWP preparation SEC(2007) 530

² As an example, the application named 'PLATO', developed by DG ENTR is housing data such as 'Commitment & Payment Forecasts over the year'. A key performance indicator to be supplied to senior management is the 'Ratio of payment execution compared to the forecast'. Payment execution data must then be retrieved from DWU (ABAC) and Forecast data from PLATO. Once retrieved in EDW, a data cleansing process is launched so that PLATO data and DWU data can communicate. The metric can then be computed, with the desired level of granularity (for instance: per month and per directorate).

³ According to DG ENTR, abnormal here has a technical meaning. It means that an indicator gives a value different from the value agreed or imposed by DG ADMIN, SEC GEN, DG BUDG, etc. acting as "master DGs".

Moreover, it considers that it deals with the implementation of the Treaty, the e-Europe Action Plan, including the derived policy measures and actions on e-Government, and the e-Commission implementation strategy based on actions 7, 8 and 9 of the Commission Reform White Paper called for a modern & efficient infrastructure including equivalent office automation technology. DG ENTR also bases the implementation of the system on the Commission's Communication on IT Governance SEC(2004)1267 stating, on page 3 that *"Proliferation of systems has led to interoperability problems between them, i.e. inconsistent data, different information held between systems, different look and feel, difficulty of combining information held in one system with that from another etc"*. As such, DG ENTR considers that these tasks must be supported by the appropriate functionalities of modern, efficient, reliable and quality management systems.

Data Subject(s) concerned

All categories of staff (officials, temporary agents, contract agents, auxiliary staff, SNE) that work, or have worked for DG ENTR are concerned data subjects.

Categories of Data concerned

- person's information : e.g. nationality, birth date, mother tongue, grade.
- job's information : e.g. job description, job functions, absences, holidays.
- employee's career information : e.g. job assignment, administrative position, job occupation type, statutory link, mobility events
- training's information : e.g. passport map of the employee, training duration, training date, participation status
- financial information : e.g. financial roles owned by the employee in ABAC

The source data fields for COMREF, SYSLOG and ABAC were also provided to the EDPS, as well as one HTML file on the data fields in the EDW.

According to the draft privacy statement provided, the HR data collected in the EDW do not contain data that could give info on the racial or ethnical origins of a person, political opinions, religious or philosophical convictions, trade-union membership or sexual life. Moreover, it is not foreseen to integrate neither the medical nor the files used for disciplinary purposes in the EDW.

Information provided to the data subjects:

A specific privacy statement will be available on-line once the EDW is deployed in production. This privacy statement contains information on the purpose of the processing, the information which is collected, the persons who have access to the data, the security measures to protect the data, the retention period of the data and the contact information about the data controller. It also contains information on how the Human Resources data are sorted.

Rights of data subjects:

According to the notification, EDW operates purely by extracting data from other sources as ABAC, SYSLOG or COMREF. There is no way to change data in the EDW, the access is read-only for everyone who has access to the data.

The notification underlined that only if an employee for a valid reason requests that any reference to his person should be deleted, the data controller will accept and guarantee that it will be executed in due time.

Automated and manual processes

There is no manual processing involved. Every data retrieved from data providers is extracted automatically by EDW processes running on a daily basis in the evening. In a data warehouse information is not changeable by individuals.

The recipients of the data

EDW is open to authorised front line employees of resources units (HR and FIN), and only those have access to the detailed data.

Persons that will have access to EDW will access it via a single WEBI portal, whatever the type of data they want to deal with. The advantages of this solution are: a single login/password to remember, a single URL and standardised reports.

As described by the data controller, the recipients are:

- Authorised personnel of HR Unit from DG ENTR (ENTR.R.2) shall have access to HR data, at the detail of the employee.
- The Head of Unit will be granted access to HR data (access granted by HR Unit) but exactly limited to that data he has access to in SYSPER2, at the detail of the employee and limited to employees of his unit.
- The Head of Unit can delegate this right to an officer he selects.

No other staff will be granted access. Access to the EDW and any other delegation will be granted and approved by the data protection coordinator.

Storage of data

The data are stored on database servers in the data centre of DIGIT in Luxembourg.

Retention policy

Since a Data Warehouse has among other functionalities the objective to keep track of all changes and to show the history of changes, DG ENTR considers that the personal data are kept as long as the purpose of processing remains.

In its privacy statement, DG ENTR clarifies its retention policy: "*As the EDW's main goal is to provide end-users with historical and present data in order to perform (among other things) comparison between years or consolidation over years, data inside EDW will be persistent and never erased. However, it may be possible that a clean-up is performed every 10 years (the exact period for data cleaning has not been defined yet) in order to keep optimal performance on EDW's time-to-answer. (Basically: When volume of data increases, performance decreases)*".

It is also stated that the data controllers of central information systems are officially contacted and informed about the purpose of EDW, as well as about the retention policy via the notification.

Time limit to block data:

It is foreseen that one month delay has to be taken into account. In this case any reference to the person will be erased.

Security measures

EDW is hosted by DIGIT's Data Center and according to the notification all technical security measures are the responsibility of DIGIT. Reference is made to the generic notice 'DPO-1' for the IT infrastructure of European Commission by DIGIT. There is also a document including generic references to access rights policies, establishing as a general rule that access permissions on the system must satisfy the restrictions of the data owners, and be updated as those evolve.

Moreover, in the privacy statement of the system, DG ENTR states that "*... data stored in the EDW are only available in read-only mode to end-users. Only internal processes to EDW are authorized to retrieve data from operational data sources (like COMREF or ABAC) and process them before any insertion in EDW. EDW's data are stored in the data centre of European Commission at Luxembourg, hence protected by several measures of defence. These measures have been implemented by DIGIT in order to protect data integrity and confidentiality*".

3. Legal aspects

3.1. Prior checking

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 of which fall within the scope of Community law*"⁴. For the reasons described below, all elements that trigger the application of the Regulation are present.

First, *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001 are collected and further processed. This appears from the lists provided with the notification.

Second, the personal data collected undergo⁵ "*automatic processing*" operations, as defined under Article 2(b) of the Regulation (EC) No 45/2001. Indeed, the personal data such as personal identification data (family name, first name), job's information, employee's career information and training's information are processed by automatic means.

Finally, the processing is carried out by a Community body, the European Commission, in the framework of Community law (Article 3(1) of the Regulation (EC) No 45/2001). Therefore, all the elements that trigger the application of the Regulation are present in this data processing.

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*

⁴ See Article 3 of Regulation (EC) No 45/2001.

⁵ Before the deployment of the interface, the reconciliation is done manually by individual auditor staff.

subject by virtue of their nature, their scope or their purposes". Article 27(2) contains a list of processing operations that are likely to present such risks, for example "processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes" (Article 27(2)(c). Indeed EDW allows interconnections not provided for under national legislation or community between data processed for different purposes.

Since prior checking aims at addressing situations that are likely to present certain risks, the opinion of the EDPS should be given prior to the start of the processing operation. The current opinion constitutes a **true prior check**. Therefore, such processing should not be implemented until the recommendations of this opinion are taken into account and the EDPS is informed of the measures of implementation.

The notification was received on 22 August 2008. Pursuant to Article 27(4) of Regulation (EC) No 45/2001, the two-month period within which the EDPS must deliver an opinion was suspended for a total of 192 days to obtain additional information. It was also suspended 15 days to allow comments on the draft Opinion. The Opinion must therefore be adopted no later than 19 May 2009.

3.2. Lawfulness of the processing

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

Of the various grounds listed under Article 5 of Regulation (EC) No 45/2001, the processing operation notified for prior checking 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 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*"

In order to determine whether the processing operations comply with Article 5 a) of Regulation (EC) No 45/2001, the first issue under Article 5(a) is to determine whether there is a specific legal basis for the processing: a Treaty provision or another legal instrument adopted on the basis of the Treaties. The second issue is to determine whether the processing operation is necessary for the performance of a task carried out in the public interest. To address this second issue in the present case, Recital 27 of the Regulation needs to be taken into account, which specifies that "*processing of personal data for performance of tasks carried out in the public interest includes the processing necessary for the management and functioning of those institutions and bodies*". Thus, the second issue in the present case is whether the processing is necessary and proportionate for the management and functioning of the European Commission (DG ENTR).

Legal basis: As described above, the legal basis of the processing presented by DG ENTR is based on several articles of the Treaty of Amsterdam (Articles 6, 7, 211, 219 and 255). Moreover, DG ENTR considers as additional legal basis the following notes and communications issued by DG ADMIN, DG BUDG, SG:

- ABM Communications SEC(2001) 1197/6&7 and COM(2003) 28;
- AAR Communication SEC(2001) 875/6 (Ref. action 82 of White paper);
- APB, APS and CLWP preparation SEC(2007) 530

Moreover, as explained above the processing deals with the implementation of the Treaty, the e-Europe Action Plan, including the derived policy measures and actions on e-Government, and the e-Commission implementation strategy based on actions 7, 8 and 9 of the Commission Reform White Paper called for a modern & efficient infrastructure including equivalent office automation technology. DG ENTR also bases the implementation of the system on the Commission's Communication on IT Governance SEC(2004)1267.

The EDPS considers the legal basis sufficiently precise to justify the processing of personal data in the context of the creation of a data warehouse.

As to the **necessity** of the processing (necessity test), according to Article 5 a) of Regulation (EC) No 45/2001, the data processing must be "*necessary for performance of a task*" as referred to above.

According to the notification, the processing operation of DG ENTR's internal system is necessary for the performance and the support of the numerous tasks carried out by the DG in the interest of the institution.

Although the necessity of supervision exists, the EDPS considers, as he already explained in previous cases⁶, that this aggregation of databases also increases the risk of "function creep" when the interlinking of two (or more) databases designed for distinct purposes will provide a new purpose for which they have not been built, a result which is in a clear contradiction of the purpose limitation principle. To be authorized such purpose must be clearly limited and the necessity demonstrated.

Therefore, the EDW should be limited to the use of data coming from internal ENTR databases and from COMREF, ABAC and SYSLOG databases and require further authorisation if other databases were to be added as database sources. Moreover, the use of data should be limited to the use specifically declared in the notification, e.g. to develop scoreboard for the management and report discrepancies of data compared to data retrieved from the original databases.

Within these conditions, the EDPS considers that the notified processing operation is lawful, as long as the institution complies with the other recommendations made in this Opinion.

3.3. Compatible use / Change of purpose

Article 4(1) (b) states that: "*Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of personal data for historical, statistical or scientific purposes shall not be considered incompatible provided that the controller provides appropriate safeguards, in particular to ensure that the data are not processed for any other purposes or used in support of measures or decisions regarding any particular individual*"

As explained in the facts, the goal of the processing operation is double: develop automatic scoreboards for supplying management metrics and investigate abnormal metrics in case there would be a discrepancy and to allow the verification of the reason(s).

When the data from the different databases (ABAC, COMREF and SYSLOG) are connected via EDW, it is in the framework of a new purpose, different from the original purposes of the

⁶ See EDPS comments on the Communication of the Commission on interoperability of European databases, 10 March 2006 available on the website.

respective processing operations, but which may be considered as compatible and acceptable with these purposes. The management in an institution is an activity falling within the general remit of a human resources department.

Article 4(1) (b) of Regulation 45/2001 provides that personal data must be "*collected for specified, explicit and lawful purposes and not further processed in a way incompatible with those purposes*". After analysis, the processing operation does not seem to entail a change in the intended purpose of the sources databases which would be incompatible with the initial purpose.

Moreover, the EDPS underlines that Article 6(1) provides that, without prejudice to Articles 4, 5 and 10 "*Personal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body*". This could be fulfilled by providing a clear and limited purpose of the processing in the privacy statement of the system.

3.4. Processing of special categories of data

After analysis of the categories of data processed, there is no evidence that DG ENTR intends to process special categories of data.

However, the EDPS notes that the privacy statement states that it is not foreseen to integrate neither the medical nor the disciplinary files in the EDW.

However, if such case was to happen, the EDPS wants to remind that the processing of 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 unless grounds can be found in article 10(2) and 10(3) for data relating to health. Moreover, according to Article 10(5), 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, subject to appropriate specific safeguards.

3.5. Data Quality

Adequacy, relevance and proportionality. Pursuant to Article 4(1)(c) of Regulation (EC) No 45/2001, personal data must be "*adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed*".

Based on the information provided to him (tables of data fields), the EDPS considers that DG ENTR should reassess its needs as regards the quantity of information it processes in the context of the EDW also in the light of the data minimization principle. Indeed, all the data fields do not seem to be necessary for the purpose envisaged by DG ENTR.

Fairness and lawfulness. Article 4(1)(a) of Regulation (EC) No 45/2001 requires that data must be processed fairly and lawfully. The issue of lawfulness was analysed above (see section 3.2). The issue of fairness is closely related to what information is provided to data subjects (see Section 3.10 below).

Accuracy. 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”.

Based on the information provided to him, the EDPS does not challenge prima facie the accuracy of the data collected through EDW, which originates from other databases. Nevertheless, where rectification takes place in one of the databases linked through EDW (see section 3.9), the quality of data in EDW could be at stake. Therefore, it should be ensured that the data which form parts of reports based on information in the EDW are accurate.

The data subject has the right to access and the right to rectify data (see section 3.9). This also makes it possible to ensure the quality of data.

3.6. Conservation of data/ Data retention

Article 4(1)(e) of Regulation (EC) No 45/2001 sets forth the principle that *"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 were further processed". "The Community institution or body shall lay down that personal data which are to be stored for longer periods for ... statistical use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subject encrypted."*

Since a Data Warehouse has among other functionalities also the objective is by definition to keep track of all changes and to show the history of changes, DG ENTR considers that the personal data are kept as long as the purpose of processing subsists. Moreover, in the light of the privacy statement, data inside EDW will be persistent and never erased.

As the EDW is meant to centralise data extracted from other databases, the EDPS considers that the retention policy of the EDW has to respect the corresponding policies of the databases from which it extracts data. It can not be allowed to grant a longer conservation period than the one authorised for the database sources. For instance, the EDPS analysed the SYSLOG processing operation (see case 2008-481), which has a specific and limited retention period. By allowing a persistent storage, the EDW would be in contradiction with the retention regime of SYSLOG. The same shall apply for ABAC and COMREF and any other database which would fill the Data Warehouse.

Moreover, the EDPS considers that if the purpose of the EDW is to manage metrics, DG ENTR should re-evaluate the possibility to render data non identifiable. In the respect of Article 4(1)(e), it is only if data are rendered anonymous that they can be stored for longer periods for historical, statistical or scientific use.

3.7. Transfer of data

The system does not foresee any transfer of data outside the institution or outside the DG ENTR. However, data are being sent by other DGs (DG ADMIN, DG BUDG,...) to feed the EDW. Therefore, there is a transfer of data within a Community institution (the Commission) according to Article 7 of Regulation (EC) No 45/2001, where DG ENTR is the recipient⁷ of the data.

⁷ e.g. authorised personnel of the H.R. Unit of DG ENTR, the respective Heads of Unit (limited to data they are authorised to access in SYSPER2 regarding their own units) and delegates of Heads of Unit have read access to the data.

In the respect of Article 7(2), *"where the data are transferred following a request from the recipient, both the controller and the recipient shall bear the responsibility for the legitimacy of this transfer"*. The text further states that: *"The controller shall be required to verify the competence of the recipient and to make a provisional evaluation of the necessity for the transfer of the data. If doubts arise as to this necessity, the controller shall seek further information from the recipient. The recipient shall ensure that the necessity for the transfer of the data can be subsequently verified."*

As a conclusion, DG ENTR, acting as recipient of the data sent by the controllers of ABAC, COMREF and SYSLOG databases, needs to justify that its competence has been verified and that the necessity for the transfer of data has been evaluated by the DGs which are controllers of the data coming from the database sources. The mere fact of contacting and informing the DPCs of these information systems about the purpose of the EDW, as it is described in the notification, is not sufficient.

Moreover, according to Article 7(3) *"The recipient shall process the personal data only for the purposes for which they were transmitted"*. In this case, the recipients should be reminded that the data cannot be used for any other purpose which is not compatible with the purposes of the EDW, as it is described in this prior-check.

The EDPS welcomes that further access to the EDW and any other delegation to services external to the recipients of the EDW may be granted and approved only after consulting the data protection coordinator. In this context, a justification of the request to access and a motivation of the data protection coordinator's approval or disapproval should be available.

3.8. Processing of personal number or unique identifier

Article 10(6) of the Regulation states that *"the European Data Protection Supervisor shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body"*.

In order to link the different databases within the EDW, it is necessary to use the data subject's staff number. Use of the staff number is justified in this case for reasons of practicality. Rather than having to enter a series of data to interconnect the systems, it can be done more readily using the staff number as an identifier. The staff number serves only to link the databases for purposes clearly set out in the project and directed towards a common end, as indicated above.

The need to use a single identifier to make connections between files thus appears to be justified and presents no specific risks given the measures to restrict access.

3.9. Right of access and rectification

According to Article 13 of the Regulation, 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.

Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data.

As explained above, EDW operates purely by extracting data from other sources (ABAC, SYSLOG and COMREF as well as internal databases of DG ENTR). It is specified that there

is no way to change a data in the EDW, the access is read-only for everyone who has access to the data. Therefore, the tool will not give access to more information than the individual source systems already provide.

Therefore, to respect articles 13 and 14, it is necessary that these rights be granted in the systems ABAC, COMREF, SYSLOG being brought together in the EDW. As EDW is a tool to access data from the other systems, access right is guaranteed. For the right of rectification, the SYSLOG system has been prior-checked by the EDPS and considered compliant regarding the right of rectification. Therefore, where applicable, the same right of rectification in the case of the ABAC and COMREF should be ensured.

Therefore, the EDPS considers that the EDW privacy statement should underline that requests for rectification regarding the data extracted through EDW should be directed to the data controllers of the respective databases.

3.10. Information to the data subject

Under Articles 11 and 12 of the Regulation, certain information must be provided to the data subject. In the case at stake, many data are not obtained directly from the data subject since the system is fed from various sources, outside the remit of DG ENTR. That said, some data may be provided by the data subject when filing forms relating to internal databases. Therefore, both Article 11 and Article 12 apply.

DG ENTR provided the EDPS with a draft privacy statement. It contains most of the elements required by Article 11 and Article 12. However, the EDPS notes that the reference to the recourse to the EDPS is missing and should be added.

As to the dissemination of the privacy statement, the EDPS considers that, besides the online publication, the privacy statement should also be personally provided to each and every staff of DG ENTR concerned.

3.11. Processing data on behalf of controllers

In the processing operation, DIGIT hosts the data which are used by DG ENTR in the framework of the EDW. As such, DIGIT should be regarded as a "processor" which processes personal data on behalf of the controller (Article 2(e) of Regulation 45/2001).

Therefore, Article 23 of Regulation 45/2001 should be taken into regard: *"The carrying out of a processing operation by way of a processor shall be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:*

(a) the processor shall act only on instructions from the controller;

(b) the obligations set out in Articles 21 and 22 shall also be incumbent on the processor unless, by virtue of Article 16 or Article 17(3), second indent, of Directive 95/46/EC, the processor is already subject to obligations with regard to confidentiality and security laid down in the national law of one of the Member States.

3. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in Article 22 shall be in writing or in another equivalent form."

In this case, DIGIT as a processor carries out its activities on the request of DG ENTR based on the legal basis explained above. Regulation 45/2001 also applies to DIGIT as it is a European body, carrying out the processing in the exercise of DIGIT's activities falling within

Community law (Article 3(1) of Regulation 45/2001). Thus, the obligations in Articles 21 on the confidentiality of processing and Articles 22 of Regulation 45/2001 on the security of processing are also incumbent on DIGIT.

Therefore, DG ENTR must adopt an agreement with DIGIT, which includes the appropriate technical and organisational measures to ensure the confidentiality and security of processing in accordance with Articles 21 and 22 of Regulation (EC) No 45/2001.⁸

3.12. Security measures

(...)

Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the considerations are fully taken into account:

- The Data Warehouse should be limited to the use of data specified in the current notification and require further authorisation if other databases were to be added as database sources;
- DG ENTR should reassess its needs as regards the quantity of information it processes in the context of the EDW in the light of the data minimization principle;
- It should be ensured that data which are part of reports based on information from the EDW are accurate;
- DG ENTR should develop a retention policy in order to respect the retention regime of the corresponding databases;
- DG ENTR should think about the possibility to render members of staff non identifiable;
- DG ENTR shall provide justification that its competence to process the data and the necessity for the transfer of data has been evaluated by the DGs responsible as controllers of the data coming from the database sources;
- The recipients of the data should be reminded that they cannot use the data for any other purpose which is not compatible with the purpose of the EDW, as described in this prior-check;
- In case of further request to access by recipients which are not covered by the notification, a justification of the request to access and a motivation of the data protection coordinator's approval or disapproval should be available;

⁸ see Opinion of 12 June 2007 on a notification for prior checking on the "Selection procedure for trainees at the General Secretariat of the Council of the European Union" (Case 2007-217) and Opinion of 28 May 2008 on a notification for Prior Checking on the engagement and use of temporary agents in the Community Plant Variety Office (Case 2008-315). Available at: www.edps.europa.eu

- The privacy statement should be personally provided to each staff member and should underline that requests for rectification regarding the data extracted through EDW should be directed to the data controllers of the respective databases;

- The privacy statement should be amended as regards the recourse to the EDPS;

(...)

Done at Brussels, 19 May 2009

(signed)

G. Buttarelli
Assistant European Data Protection Supervisor