Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Central Bank regarding the *"accident and occupational disease procedure"*

Brussels, 20 February 2014 (Case 2012-0792)

1. Proceedings

On 14 September 2012, the European Data Protection Supervisor ("the EDPS") received a notification for prior checking within the meaning of Article 27(3) of Regulation 45/2001 ("the Regulation") concerning the "accident and occupational disease procedure" from the Data Protection Officer ("the DPO") of the European Central Bank ("ECB").

Since the receipt of the notification, the EDPS had several exchanges of correspondence with the DPO for further information and clarifications regarding the processing at hand.

The draft Opinion was sent to the DPO for comments on 4 February 2014. The EDPS received a reply on 12 February 2014.

2. Facts

Purpose and Data subjects

The DG-Human Resources, Budget and Organisation ("DG-H") is responsible for the management of the procedures related to the recognition of accidents at work and occupational diseases in order to guarantee the payment of the benefits and reimbursement of medical expenses to the persons concerned.

The data subjects are the ECB's staff members (and where involved, their spouse, recognised partner or/and dependant child), the short-term contract employees, the participants in the Graduate Programme of the ECB, potential witnesses and third parties (injured or not) related to an accident.

Legal basis

The legal basis of the processing consists of:

- Articles 7,10, 16, 19, 28, 31, 32, 33 and 34 of the ECB Conditions of Employment;
- Annex IV to the ECB's Conditions of Employment and
- Articles 12, 27, 28, 29 and 30 of the ECB Conditions of Short-Term Employment.

Procedure and data processed

The initial collection of information is manual and paper based, such as the doctors' reports. This information is scanned in a software database.

In case of an accident at work or an occupational disease, data subjects should submit the accident notification form or the application for recognition of an occupational disease to the Health and Safety function in DG-H.

They should also submit a medical certificate and any other supporting documents to the ECB's medical adviser in a sealed envelope. The Director General of the DG-H or their deputy, on the basis of expert medical opinion of one or more doctors (either ECB's medical service or external ones), takes the final decision related to the recognition of an accident at work, of the occupational nature of a disease and the establishment of the degree of permanent invalidity after consolidation of injuries.

The ECB's medical adviser and external doctors are independent medical experts and are subject to the EU member state's legislation of the country where they work. For instance, in Germany they are bound by a contractual and statutory regime imposing strict confidentiality and professional secrecy obligations on them under Article 203 (1) No. 1 of German Criminal Code (StGB). They are officially appointed by the Director General of the DG-H or their deputy (and/or by the President of the Medical Association of the state of Hessen in case of appeals (Hessische Landesärztekammer) issuing "*The letter of appointment of medical expert(s)"*. There is an implicit contract between the ECB and the external doctors (medical experts) concluded by "*The letter of appointment of medical expert(s)*" covering the data protection aspects (which refer to Article 10 of the Regulation).

There is no direct communication between the appointed external doctors and the DG-H beyond purely administrative elements of the procedure, namely submission of documents, payment of expenses, etc. The external doctors/experts communicate their medical findings to the ECB Medical Adviser. On the basis of these medical findings, the ECB Medical Adviser prepares non-confidential information to the persons in charge of the Health and Safety function in DG-H.

In case of an appeal procedure, the Medical Committee (under Article 6.6 of the ECB Staff Rules), on completing its deliberations, adopts its opinion in the form of a medical report. The Medical Committee also provides a summary containing non-confidential information from this report to the persons in charge of the Health and Safety section in DG-H.

In case of non-work related accidents, the injured persons should submit a claim to an **external insurer**, **via an external administrator**. The insurer's tasks are limited to dispute settlement and to risk carriage. The external administrator provides the DG-H with non-confidential information on accidents sustained by the data subjects for statistical purposes, contract management and procurement, namely: 1) which staff members reported the accident, 2) when the accident took place, 3) the category of accident, 4) if the accident resulted in permanent disability and, if this is the case, the level of compensation and 5) if applicable, rejection and reasons for rejection to recognise an accident. The ECB concluded a contract with the external insurer and the external administrator, who are both subject to one of the EU member states' legislations and the contract includes data protection, confidentiality and security provisions.

In addition, the ECB concluded a contract with **another external administrator** for the reimbursement of medical expenses as part of the ECB's medical benefits and dental plan. The external administrator receives directly from the staff members a claim form for reimbursement of medical expenses, accompanied with invoices and he reimburses the data subjects. The contract is subject to one of the EU member states' legislations and it includes data protection, confidentiality and security provisions.

Other data processed

Apart from administrative and accident related data of the data subject, the accident notification form requires also to enclose the police report, if available, the name and address of the witness(es) and the name, address and insurance company of a third party involved in an accident either injured or not.

Furthermore, the claim for reimbursement of medical expenses, requires, inter alia, the name of the spouse, recognised partner or/and dependant child in case they have been also injured in an accident with the staff member.

All persons in charge working at the Health and Safety section in DG-H as well as the persons working in the ECB's medical centre signed confidentiality statements, which state that they are bound by professional secrecy obligations. These confidentiality statements make also reference to provisions of the Regulation.

Recipients

According to the above procedure, the recipients of the data processed are the following:

External

- ECB's medical adviser who receives all medical certificates and history of medical checks of the data subjects as well as the application form for recognition of an occupational disease;
- the external doctors receive the same information as the ECB medical advisor;
- the external insurer of the accident insurance scheme, who receives via the external administrator an accident or occupational disease notification form, supporting medical certificates after the medical visit, medical certificates issued in the course of the accident at work and occupational disease procedure relevant for the stabilisation of the medical condition and medical certificates for the determination of a permanent degree of invalidity;
- the external administrator of the ECB's medical benefits and dental plan, who receives a claim form for reimbursement of medical expenses, accompanied with invoices from the staff members.

RightS of access and rectification

Data subjects may have access to their medical data held by the ECB's medical adviser and make copies of them. They may also have access to their personal data held by the DG-H.

They also have the right of rectification and the right to submit to their medical file counter-opinions by another doctor or a relevant Court decision in this regard.

Right of information

The privacy statement for health related data refers to some of the information listed in Articles 11 and 12 of the Regulation.

It is inserted in all forms (Accident at work notification form, Non-work related accident notification form, Application for recognition of an occupational disease) that are publicly accessible on intranet.

Retention policy

All administrative and financial data are kept in the personal files for a maximum of 10 years after the staff member's employment with the ECB has ceased or after the last pension payment.

Medical certificates and health related documents in the context of accident and occupational diseases are kept for a maximum of five years starting from the date of their submission.

Medical paper files are kept for a period of 30 years upon closure of the file. Data contained in the **medical software** will be stored for a period of 10 years upon closure of the file.

As the ECB DPO explained that, for the time being, the ECB rules on retention do not specifically address the medical file in paper but more generally personal data. As regards the retention period of the medical file, the ECB has initiated the procedure for amending the ECB Staff Rules on the retention period of medical files. The retention period of the medical data kept in paper form will be adjusted with the medical data kept in electronic form.

According to the notification, further processing for historical, statistical or scientific purposes is not envisaged. However, as it is stated above in page 2 and on the basis of further information from the controller, the external administrator provides DG-H annually aggregated anonymous data on insurance cases and insurance benefits for statistical, contract management and procurement purposes.

Storage and security measures

Medical files are stored in locked cabinets (fireproof cupboards) within the medical service of the ECB. Medical data will also be stored in electronic form in the medical software and it will contain all additional medical reports, the ECB's medical adviser's reports and the final decision taken by the Director General of the DG-H or Deputy. Access to the medical file of the data subject and the medical software is only available to the medical adviser and nurses. The electronic data are encrypted in the database and the users as well as any changes must be approved and authorised by the ECB's medical centre.

The accident notification form, the sick leave notes issued by the ECB's medical adviser or other doctor, the application for recognition of an occupational disease and the final decisions taken by the Director General of the DG-H are kept separately in a special section of the personal file. Access to the section is granted only to the persons in charge of the Health and Safety function of the DG-H. Personal files are stored in safe cabinets.

3. Legal aspects

3.1 Prior checking

Applicability of the Regulation: The processing of data under analysis constitutes a processing of personal data ("*any information relating to an identified or identifiable natural person*"-Article 2 (a) of the Regulation). The data processing is performed by an institution of the European Union, the ECB, in the exercise of activities which fall within the scope of EU law[1]. The processing of the data is both manual, which forms part or intended to form part of a filing system (medical reports, medical files), and automatic (information is introduced in a software database). The Regulation is therefore applicable.

Grounds for prior checking: Article 27 (1) of the Regulation subjects to prior checking 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*" by the EDPS. Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks. According to Article 27(2)(a) of the Regulation "*the processing of data relating to health*" is subject to prior checking by the EDPS, which is the case here as the data fall within the scope of data concerning health.

Notification and due date for the EDPS Opinion: The notification of the DPO was received on 14 September 2012. Since the date of receipt, the EDPS had several exchanges of correspondence with the DPO for further information and clarifications about the processing at hand. As this is an ex-post case, the deadline of two months for the EDPS to issue his Opinion does not apply; this case has been dealt with on a best-effort basis**.**

3.2 Lawfulness of the processing

According to Article 5 of the Regulation, data may be processed only on one of the grounds specified.

Of the five grounds listed in Article 5, the processing under analysis satisfies the conditions set out in Article 5(a) of the Regulation, to the effect that data may be processed 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* (...)'.

In the present case, **the legal basis** for the processing is found in the legal provisions of the ECB's Conditions of Employment indicated in the facts.

The necessity for processing is also mentioned in paragraph 27 of the preamble to the Regulation, which states that "*Processing of personal data for the performance of tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies*". The processing of personal data at stake is necessary for the management of the payment of benefits and reimbursement of medical expenses to the data subjects related to accidents at work and occupational diseases. This processing therefore contributes to the sound management of human resources and the functioning of the ECB.

[1] The concepts of "Community institutions and bodies" and "Community law" can not be any longer used after the entry into force of the Lisbon Treaty on 1st December 2009. Article 3 of Regulation 45/2001 must therefore be read in light of the Lisbon Treaty.

3.3 Processing of special categories of data

Article 10(1) of the Regulation states that the processing of personal data on health is prohibited, except where it is justified by reasons provided in Articles 10(2) and 10(3) of the Regulation.

Article 10(2)(b) applies in this case: "*Paragraph 1* (prohibition of the processing of data on health) *shall not apply where … processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof...*". The processing under analysis is necessary in order to comply with the specific obligations and rights of the ECB, as an employer, under labour law. The ECB therefore carries out this processing in accordance with the provisions of its Conditions of Employment pursuant to Article 10(2)(b) of the Regulation.

In addition, according to the notification all persons in charge working in DG-H as well as the persons working in the ECB's medical centre are bound by professional secrecy obligations through confidentiality statements. Article 10(3) of the Regulation is therefore respected.

3.4 Data Quality

Adequacy, relevance and proportionality: According to Article 4(1)(c) of the Regulation, personal data must be "*adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed*". It should therefore be verified that the data collected are relevant in relation to the purpose for which they are being processed.

The data described in this Opinion seem to satisfy these conditions regarding the purpose of the processing explained above.

Accuracy: Article (4)(1)(d) of the Regulation provides that data must be *"accurate and, where necessary, kept up to date*". According to this Article, "*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*".

In the present case, the procedures in place, enables one to conclude that the system itself gives a reasonable guarantee of data quality. However, the EDPS notes that medical data in paper file have a different retention period than medical data in electronic form. There might be a risk that due to different retention periods of the same data in different forms the accuracy of the data subjects' medical data might not be fully guaranteed. The EDPS therefore recommends that the ECB takes all reasonable steps to ensure that the principle of accuracy under Article 4(1)(d) of the Regulation is respected (see further on retention period, point 3.5).

As to the rights of access and rectification, they seem to be available to the data subject, in order to make his personal data related to accidents and occupational diseases as comprehensive as possible. These rights constitute the second means of ensuring that data concerning the data subjects are accurate and updated (see further on the right of access, point 3.7).

Fairness and Lawfulness: Article (4)(1)(a) of the Regulation provides that personal data must be *'processed fairly and lawfully'*. The lawfulness of the processing has already been

discussed in section 3.2 of this Opinion. As to fairness, this is linked to the information that must be provided to the data subject (see further on the right to information, point 3.8).

3.5. Conservation of data

Article 4 (1) (e) of the Regulation states 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 are further processed*".

The EDPS considers that the retention periods of administrative and financial data as well as medical certificates related to the processing at hand are reasonable and necessary for the purposes for which they were collected and further processed in light of Article 4(1)(e) of the Regulation.
Moreover, the EDPS welcomes the ECB's initiative for amending its Staff Rules on the retention period of medical files and for harmonising the retention period of medical data in paper with the medical data in electronic form. The EDPS invites the ECB to take into consideration the EDPS Guidelines on the processing of health data at workplace[2], where the EDPS recommended that medical files paper and/or in electronic form should be kept for a maximum period of 30 years after the last medical document is inserted in the file. Furthermore, the EDPS highlighted that the nature of the medical documents should be examined in light of their purposes and the rules applicable in order to determine what retention period would be suitable and necessary to each type of document. The EDPS recommends that the ECB adopts a retention period for medical files in light of the Guidelines.

Finally, the EDPS notes that, neither the notification nor the privacy statement, indicate clearly all retention periods as described in the facts of the present Opinion. The EDPS recommends that the ECB updates both documents accordingly.

As to the issue of aggregated anonymous data, the EDPS notes that the notification does not state the correct information as it mentions that no further processing is envisaged for statistical purposes. The EDPS therefore recommends that the ECB indicates in the notification that the external administrator provides DG-H annually aggregated anonymous data on insurance cases and insurance benefits for statistical, contract management and procurement purposes.

3.6 Transfer of data

Articles 7, 8 and 9 of the Regulation set forth certain obligations that apply when controllers transfer personal data to third parties. The rules differ depending on whether the transfer is made (i) to or within EU institutions or bodies (based on Article 7), (ii) to recipients subject to Directive 95/46/EC (based on Article 8), or (iii) to other types of recipients (based on Article 9).

External transfers
The ECB concluded contracts with its medical advisor, other external doctors, an external insurer and an external administrator and according to their contracts they are all subject to

[2] https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Guidelines.

one of the EU member states' legislations implementing Directive 95/46/EC. This means that Article 8 of the Regulation is applicable. The EDPS considers that the transfer of data, as indicated in the facts, is necessary to the above recipients for the performance of their respective tasks carried out in the public interest under Article 8(a) of the Regulation.

3.7 Rights of access and rectification

Article 13 of the Regulation provides for the principle of the right of access to the data –and the procedures thereof– at the request of the data subject. Article 14 of the Regulation provides for the data subject's right of rectification.

Both the notification and information note make reference to the existence of both rights and they explain how data subjects can exercise these rights. The ECB also indicates the meaning of the right of rectification in the context of the processing of health related data.

Nevertheless, the EDPS draws the attention of the ECB to Article 20 of the Regulation, which lays down certain restrictions on this right, in particular where such restrictions constitute a necessary measure for the protection of the data subject or of the rights and freedoms of others. For instance, Data subjects may exercise their right of direct access to their medical file, on the premises of the ECB's medical service in the presence of a person designated by the medical service. In case of psychiatric/psychological reports, data subjects may consult them through the intermediary of a doctor appointed by the data subject. As to the doctors' personal notes, data subjects may not have access to them if, under the terms of Article 20(1)(c) and on the basis of a case-by-case examination, this restriction is necessary to guarantee the protection of the data subject or the rights and freedoms of others.

The EDPS therefore recommends that the ECB explains in the information note the possibility of the application of Article 20 of the Regulation restrictively in exceptional cases. The EDPS invites the ECB to examine a potential restriction on access to medical files on a case-by-case basis in accordance with the principle of proportionality. Article 20 of the Regulation must not result to a general refusal of access to the personal notes of doctors in the medical file.

3.8 Information to the data subject

Articles 11 and 12 of the Regulation relate to the information to be given to data subjects in order to ensure transparency in the processing of personal data. In the present case, some of the data are collected directly from the data subject and others from other persons (i.e doctors, DG-H officials, insurer, administrator, potential witnesses or injured third parties).

In the case at hand, the privacy statement sets out most of the items included in Articles 11 and 12 of the Regulation. However, the EDPS recommends that the ECB adds to the privacy statement the following information:

- retention periods of all types of personal data processed, as explained in point 3.5 of the Opinion;
- clarifications on the right of access, as analysed in point 3.7 of this Opinion.

Furthermore, the EDPS notes that in case of an accident, the ECB might process personal data of potential witnesses and third parties (injured or not) related to an accident. The ECB, as a

controller of the processing at hand, has therefore an obligation under the Regulation to inform these data subjects, where the data have been obtained from them. The EDPS recommends that the ECB prepares a short privacy statement in conformity with Article 11 of the Regulation and adds to the notification these categories of data subjects, as potential data subjects when an accident occurs[3].

3.9 Sub-contracting

Article 23 of the Regulation provides that, when a processing operation is carried out on behalf of the controller, the latter should ensure that its processor can provide sufficient guarantees in respect of technical and organisational security measures for the processing of the personal data.

In the present case, all external contractors are bound by contracts with the ECB governed by EU legislation implementing Directive 95/46/EC and which specifically include data protection, confidentiality and security provisions. The ECB is therefore in compliance with the requirements under Article 23 of the Regulation.

3.10 Security Measures

According to Article 22 of the Regulation concerning the security of processing, *"the controller shall implement 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 should 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.

After review of the security measures described in the notification, there is no reason to believe that the measures implemented by the ECB do not comply with Article 22 of the Regulation.

4. Conclusion

There is no reason to believe that there is a breach of the provisions of the Regulation, provided that the following considerations are taken into account. In particular the ECB should:

- take all reasonable steps to ensure that the principle of accuracy in medical files both paper and electronic form, namely harmonise the retention period of medical data in paper with the medical data in electronic form;

- adopt the retention period of medical files as recommended in the EDPS Guidelines;

- indicate in the notification that the external administrator provides DG-H annually aggregated anonymous data on insurance cases and insurance benefits for statistical, contract management and procurement purposes;

[3] See EDPS Opinion of 27 June 2012 on the Council's notification regarding "Gestion du Bureau Véhicules de Service", case 2012-0157.

- explain in the notification and privacy statement, the possibility of the application of Article 20 of the Regulation regarding the right of access to the medical file. The ECB should ensure that restrictions on access to medical files are examined on a case-by-case basis in accordance with the principle of proportionality;

- include in the privacy statement the information as explained in point 3.8 of this Opinion;

- prepare a short privacy statement for potential witnesses and third parties (injured or not) related to an accident and adds them as an additional category of data subjects in the notification.

Done at Brussels, 20 February 2014

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor