Opinion on a notification for prior checking received from the Data Protection Officer of the European Investment Bank *on the modification of the data processing operations concerning "gestion du temps" and "medical records"*

Brussels, 3 August 2007 (Case 2007-373)

1. Proceedings

On 17 January 2007, the Data Protection Officer (DPO) of the European Investment Bank (EIB) consulted the European Data Protection Supervisor (EDPS) about the request of the "*médecin de travail*" (physician) of the EIB to have access to the data on "absences without medical certificates". This consultation concerns an already prior checked notification (medical records and services management, 2005-396) and is also related to another notification (time management, 2004-0306).

After several exchanges, on 26 April 2007, the EDPS gave his answer on the consultation by the DPO. He requested modified notifications on "medical records" and on "time management" (explaining how the latter system would change in the light of the modifications on the processing operation concerning the "medical records").

On 4 June 2007 the DPO submitted for prior checking the two modified notification forms. On 17 July 2007, the EDPS sent the draft opinion to the DPO with a request to comment on it. EIB commented on 2 August 2007.

2. The facts

The notified processing operation constitutes a true prior check. In order to monitor staff health and with a focus on early prevention of health risks, it is planned that the physician at the Occupation Health Centre (OHC) of the EIB will have access to all data related to uncertified sick leave. Leaves without medical certificates can last up to a maximum of three consecutive days, and at present no data relating to them are accessible by the physician.

EIB raised the following arguments to justify the necessity of access by the physician: a series of small not certified repetitive absences could signal a developing disease which the staff member does not interpret correctly or ignores, and therefore, in the context of taking preventive measures and in the context of the employer's responsibility towards the actual and future health of the employees, the physician needs to have access to those indicators on absences. Absences without medical certificates will be used to complete a dossier on individual absences, which is needed in the context of the medical history of the staff member and falls under medical secrecy. Without the possibility of accessing that type of sensitive data by the physician, prevention on an individual level could only start when symptoms of a real disease are clearly exhibited. However, by using the data regarding uncertified sick leave the development of certain diseases may be prevented.

Data related to uncertified sick-leaves, collected by the "Gestion the Temps" (time management) application, is accessible via a secured IT tool. The additional access planned to be granted under this notification is limited to the OHC.

3. Legal aspects

3.1. Grounds for prior checking

The case concerns access by the EIB physician to personal data contained in the "time management" system regarding sick leaves without medical certificates. The processing is to be carried out in the context of the activities of the EIB, a Community institution, in its exercise falling under Community law. Therefore, the case falls under Article 3(1) of Regulation (EC) No 45/2001 (Regulation). It concerns data on leaves entered manually but processed by automated means in the "time management" system. The data are subsequently placed by the physician in the data subjects' medical dossiers. Thus the case falls under Article 3(2) of the Regulation.

The notification concerns health related data, and therefore, the case should be prior checked pursuant to Article 27(2)(a) of the Regulation.

The notification of the DPO was received on 4 June 2007. According to Article 27(4) of the Regulation this opinion must be delivered within two months, that is, by 5 August 2007. The procedure was suspended for 16 days which was used by EIB to comment on the draft EDPS opinion. Thus, the opinion should be delivered no later than 21 August 2007.

3.2. Lawfulness of the processing

Article 5 of the Regulation allows for the processing of personal data only on specific grounds. Article 5(a) of the Regulation allows for the processing of personal data if that 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".

The EDPS considers that the *necessity* and *proportionality* of the EIB physician's access to the data on uncertified medical leaves are questionable.

The justification given to the EDPS in the course of the consultation phase of the EDPS procedure was that such access serves as a disease prevention measure on individual level. The EDPS acknowledges that prevention is a legitimate concern and also recognizes that medical professionals have a considerable degree of discretion in defining what data can be useful for purposes of prevention. The EDPS is also willing to accept that there may be some utility in providing access to the data on the number of uncertified sick days to the OHC physician, although he raises doubts about the accuracy and actual usefulness of the data obtained as noted below in point 3.5.

With that said, the concern for prevention must be balanced with the right to privacy and medical self-determination of the patient. The EIB Staff Regulation allows taking a maximum of twelve days off per year without obtaining a medical certificate, and thereby foregoes a control by a physician of whether the staff member was indeed so sick that it justified his or her absence from work. So long as the system and the EIB Staff Regulation continue to provide for this opportunity without further restrictions, EIB cannot curb this right by

routinely requiring the staff member to provide further explanations how he or she used the days taken off as medical leave without certificate, whether for human resources purposes or for purposes of medical prevention.[1]

To accommodate the interests of individual prevention, which the EDPS understands is the sole reason for the requested access to data by the OHC physician, while at the same time ensuring the safeguard of staff members' right to privacy, the EDPS recommends that EIB ensures that each staff member remains free to decide whether he or she should give access to the OHC physician to data concerning his or her uncertified medical leaves. The consent must be "unambiguous" as per Article 5 (d)) and "express" pursuant to Article 10(2)(a) of the Regulation.

Finally, there is no internal rule specifically authorising the physician at the OHC to access data on sick leave without medical certificates. Article 27 of the EIB Staff Regulation provides for "a medical examination carried out at any time during the illness"; however, this appears to apply only to leaves with medical certificate. On internal rules, see also point 3.4 below.

3.3. Processing of special categories of data

Personal data revealing data concerning health is prohibited unless grounds can be found in Articles 10(2) and/or 10(3) of the Regulation. Due to the sensitivity of the data concerned, exceptions should be interpreted narrowly.

Article 10(3) of the Regulation allows for the processing of health data where it is required "for the purposes of preventive medicine, medical diagnosis (...) and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy."

The requirements of this Article are twofold: 1) the processing should be *required* for medical diagnosis, and 2) data should be processed by a physician bound by medical secrecy. The first requirement has been discussed under point 3.2 (lawfulness). The second one is met in the proposed processing operation as it is a physician who accesses data on leave without medical certificates.

As to the consent of data subjects under Articles 5(d) and 10(2)(a) of the Regulation, the authorization can be given, for example, via a declaration made during the first annual medical check-up that the staff member participates in after the date of this Opinion. This may take a similar form to requesting consent for AIDS tests. However, EIB is free to choose the timing and the method for obtaining consent. The EDPS has no objections, for example, if EIB decides to circulate an email requesting written consent, or if employees give consent by other electronic means, such as by making their own entries in a database that the EIB uses. In any event, when requesting consent, it must be ensured that the staff member clearly understands that consent can be withheld or subsequently withdrawn at any time, without any justification, and with no adverse consequences. It must also be made clear that providing this information will only serve the purposes of prevention.

[1] This Opinion does not cover the issue of whether and to what extent staff members can be required to account for the use of uncertified days in case of suspicion or proof of abuse of the system (e.g. staff members who use their sick leaves to run errands in town or go on holidays).

During the annual medical exams, the OHC physician (or the medical practitioner chosen by the staff member) can also, with the freely given consent of the staff member, enquire about the frequency of these short term absences, and ask additional questions relating to the reasons for such absences, provided that the staff member is willing to engage in that discussion.

Based on the foregoing, the EDPS considers that only obtaining the unambiguous and express consent of the staff member can make the processing lawful under Articles 5(d) and 10(2) of the Regulation.

3.4. Change of purpose/incompatible use

Article 4(1)(b) of the Regulation requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Article 6(1) of the Regulation requires that 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.

Data on sick leave without medical certificates are collected and processed by the "time management" system for the purposes of managing absences. If those data are to be accessed and used by the physician of the EIB for health purposes, notably for disease prevention on the individual level of the staff members, a clear change of purpose occurs as those data are collected in the framework of time management. Therefore, such a change of purpose should be expressly authorised by the internal rules of the EIB. This is currently not the case.

3.5. Data Quality

Article 4(1)(d) of the Regulation requires that personal data must be accurate and where necessary kept up to date.

The EDPS does not see how the accuracy of the health data is ensured for this processing operation. The "time management" system will only contain the number of days an individual entered concerning sick leave without medical certificates. This is very vague general information. The EDPS does not challenge the statement by the physician that small repetitive absences may constitute symptoms of a more serious disease. It is for the medical professional to draw the appropriate conclusions. However, the EDPS points out that the data entered on the "time management" system can, in any event, only serve as a very distant, inconclusive, and unreliable indicative of any medical problems that a staff member might have. Therefore, it may be misleading to draw general conclusions from the number of days an employee takes off as uncertified sick leave, and may be dangerous to build a prevention program based on these potentially misleading statistics.

4. Conclusions

Based on the foregoing, the EDPS believes that the EIB would be in breach of the above described provisions of the Regulation unless it ensures that staff members are requested to provide their freely given, unambiguous consent to the OHC physician's access to data regarding their uncertified medical leave. When requesting consent, it must be ensured that the staff member clearly understands that consent can be withheld or subsequently withdrawn at any time, without any justification, and with no adverse consequences. It must also be made clear that providing this information will only serve the purposes of prevention.

The information provided to data subjects and the internal rules and documents drawn up regarding both the time management system and the medical filing system must also be modified accordingly.

Done at Brussels, 3 August 2007

Joaquín BAYO DELGADO
European Data Protection Assistant Supervisor