**Prior checking opinion on the management of absences and sickness leave using the "Centurio" database at the Economic and Social Committee ("EESC") notified on 3 November 2009**

Brussels, 5 March 2010 (joint cases 2009-0702 and 0703)

## 1. Proceedings

On 3 November 2009 EESC notified the European Data Protection Supervisor ("**EDPS**") of the two related processing noted above for "ex-post" prior checking. On 11 December 2009 the EDPS requested a meeting to clarify some of the facts and view Centurio on-line. At the same time, the EDPS also sent EESC a summary of the facts, and a set of questions to be discussed at the meeting. The meeting took place on 13 January 2010. On 26 January 2010, the EDPS sent EESC the draft Opinion. EESC commented on 26 February 2010.

## 2. The facts

The prior checking covers the data protection aspects of the management of absences and sickness leave at the EESC and the operation and use of the "Centurio" IT system for this purpose. The EDPS opinion focuses on special leave, medical leave and maternity leave but when necessary also addresses other aspects of the management of absences.

The procedures are carried out on the basis of Articles 57-60 as well as Annex V of the Staff Regulations and Articles 16 and 91 of the Conditions of Employment. EESC also adopted several formal internal decisions to put the procedures into effect:

- Decision nr 477/04/A on medical leave,
- Decision nr 201/04 A on annual and special leave and
- Decision nr 104/09/A on national experts.

Any absence is first recorded in the "list of presence" module of the Centurio database directly by each unit, typically by one or more assistants designated for this purpose by the head of unit. Each manager has on-line access to the list of presence of his or her own staff. Managers may also authorize access "in the interest of the service" to any of their staff. This access is typically given to those inputting the data into Centurio. Usually this means one or two assistants, but on occasion, many more persons have access as staff in certain units take turns in inputting data. The implementation of granting access rights will then be carried out by the IT service.

The "list of presence" is, in fact, a calendar, which indicates, for each staff member, and for each day, whether he or she is present at the office, or absent, and on what ground. The list of

presence uses a colour and letter coding. These codes indicate, for each day, whether the person is present at the office, or whether he is away on one of the following grounds:

- annual leave,
- mission,
- training,
- coaching,[1]
- medical leave,
- maternity leave,
- parental leave,
- family leave,
- strike,
- recuperation of overtime,
- recuperation of flexible working hours,
- special leave,
- part-time work, or for
- unknown reason.

There is no further breakdown on the list of presence. Further details, however, are encoded into the database by the "Leave and Overtime" department ("**competent department**") in the human resources unit ("**HR unit**")[2] and by the medical service of the EESC when these services "validate" the absences, typically based on supporting documents submitted by the staff member concerned. Certain subcategories for medical leave are indicated by the medical service when encoding certificates in the "Medical follow up" module. Most subcategories for all other types of absences including special leave and maternity leave are encoded in the individual's calendar by the competent department, although confirmation of missions and training is the responsibility of these latter departments.

Altogether, there are nearly 60 different subcategories and corresponding letter and colour codes used in Centurio for the management of absences and sickness leave, although some of these subcategories are infrequently used and some are obsolete. Of these subcategories, 23 relate to different types of special leaves, and 7 relate to different types of absences due to medical reasons. Some examples are as follows:

For special leave, the competent department encodes whether the leave was granted, for example, due to serious illness or death of spouse, a child, or a relative in the ascending line, on account of adoption, to attend EPSO exams, a medical consultation, or to participate in an election, get married, or attend the wedding of a child. For medical leave, the subcategories encoded into Centurio include medical leave without a doctor's certificate (in case of short absences subject to an annual maximum of 12 days), medical leave with certificate, part-time employment for medical reasons, medical consultation, accidents, hospitalization, and others. There is also a category for unauthorized absence (Article 60 of the Staff Regulations). This latter is encoded by the competent department.

Subcategories that are not related to special leaves or medical leave also show a great variety. Some of these are closely related to the performance of one's duties such as subcategories

[1] This is, in fact, not an "absence" code, but an indication to the department (Translation) that this person is not available for his/her usual tasks and thus not included in the statistics of pages translated/dept/month.

[2] The competent department currently consists of a team of three individuals, each of whom has read and write access to all data on absences and medical leaves in Centurio. The head of the HR unit and his/her assistant has the same access rights to data in Centurio. The same persons also have access to the paper files (except for the medical certificates, which are held by the medical service).

related to missions and training. Other subcategories indicate whether absences were, for example, due to "annual holidays" or "flexitime compensation". Some other information included in the absence database are of potentially more sensitive nature: for example, the detailed subcategories show whether the employee was on strike, whether he or she took off time for family leave, was away on account of a "very serious illness" of a child, on parental leave, or on leave for trade union business.

Requests for special leave are submitted on a paper form by staff members to their heads of units. Any supporting documents are submitted directly to the competent department. Medical documents are submitted to the Medical Service which then provides the competent sector with authorisation for the absence requested. The supporting documents may be, among others, death certificates; convocations before a tribunal; authorizations by the EESC medical service in case of illness of relatives[3]; or doctor's certificates in case of a medical consultation. The requests are then transferred to the competent department, which will ultimately store both the requests and the supporting documents. This is with the exception of medical certificates, which are always held by the medical service only.

Staff inform their unit of any absence for illness, typically by telephone, text message or email, and this is then indicated in the "list of presence". The supporting documents (medical certificates) are provided directly to the medical service and will continue to be held by the medical service. The information on the type of medical leave (for example, whether the medical leave is certified, due to an accident, etc), is entered directly by the medical service, via the module "medical follow-up".

As the competent department, the medical service, composed of the Committee's doctor, the nurse, two welfare assistants and the secretary, also has access to all data in Centurio related to absences. This means, first of all, that the medical service has access not only to medical leave information but also to data about other types of absences, for example, to data about special leave. Second, the medical service not only has access to data on the list of presence but also to the detailed subcategories.

Heads of units have access to all absence data of their own staff. This includes first of all the list of presence, which is typically used to check availability of a particular employee at the present time or in the future, for planning purposes. However, via the calendar function, heads of units, if they wish, can also consult the detailed subcategories of any of their staff. This also includes historic data going back several years (subject to the limits of the retention period that will be described below).

Further, there is also a module in Centurio where any staff member can view the organisational structure of the EESC, as well as a directory of all staff. The staff directory indicates not only the name, job title and contact information (location of the office, work email and work telephone) but also indicates whether a staff member is on a contract or a permanent official. Further, there is a possibility to upload a photo. This has initially been based on individual opt-in consent, but for recently recruited staff members the practice has become to automatically upload the ID picture taken for the badges used for access control.

The staff directory also shows whether the staff member is present or absent from the office on the day when the directory is consulted. This feature was introduced to facilitate reaching and finding a person, or their back-up person at the office. On the page which brings up the person's contact information in case the person is absent a red warning appears noting that the

[3] The authorization contains no health-related data other than the name of the relative who is ill and the fact that he/she is ill; importantly, there is no information regarding the nature of the illness.

person is "absent today". There is no feature to indicate when the staff member returns to the office.

Information on data protection is given to the individuals in the following ways:

- the formal decisions of the EESC implementing the Staff Regulation and the Conditions of Employment do not explicitly address any data protection issues but they do make it clear what the legal basis and the purposes of the processing are and that the processing is carried out by the EESC;
- two relevant and separate data protection notices are available on the EESC intranet, one on absences and presence and another one on medical leave, both easily available from the pages containing information regarding the rules on absences;
- a shorter data protection notice is also included on the forms on which a staff member needs to request a particular type of leave (e.g. special leave ).

Staff members also have direct read-only access to consult their own data in Centurio via the "consultation module": they can thus see what data are processed about them and verify their accuracy. To further increase accuracy of the data, once a year staff members are invited to formally verify and confirm the accuracy of recent data available in Centurio. This does not include all data, for example, all medical leave granted throughout the year, but does include certain main items which required a formal decision by the Appointing Authority, such as whether the person at the time of the declaration is still on parental or family leave.

The consultation of the paper files is made upon simple request to the competent department. Blocking and erasure are carried out within 15 days upon request. Correction of the data in Centurio is made on simple e-mail request, usually within one day, or at most, within a week.

Both the paper files and the data uploaded onto Centurio are held for five years, with two exceptions noted below. The main reason for keeping the medical leave data for five years is to allow the necessary calculations to be made in the invalidity procedure: Article 59(4) of the Staff Regulation allows the appointing authority to initiate an invalidity procedure for an official whose sick leave totals more than 12 months in any period of three years. Data are deleted from Centurio only once a year, in January-February, simultaneously with the deletion of the corresponding paper files. EESC explained that for this reason a slightly longer period, up to at least four years, is necessary. To illustrate, this allows that if a period of medical leave occurred in March 2007, the information would be deleted in January-February 2011 rather than January-February 2010, and thus, would be still available until and including February and March 2010, when it may still be necessary for the calculations. To ensure the availability of data as a contingency for unexpected occurrences, EESC established a slightly even longer period, five years.

The exceptions are as follows:

- leave on personal ground: data are retained for the entire career of the person to keep track when the total time granted reaches the maximum permitted 15 years (Article 40(2) of the Staff Regulations);
- family leave: data are retained for the entire career of the person to keep track when the total time granted reaches the maximum permitted nine months (Article 42(b) of the Staff Regulations)

EESC also keeps non-identifiable personal data beyond the normal retention period for statistical purposes.

When officials are transferred to another institution, their annual leave and special leave data for the current calendar year are also transferred, along with their personal files, but only in paper form (when officials are transferred to the Committee of Regions, their data in Centurio are also transferred). Data are similarly transferred when a temporary agent or contractual agent is transferred to the Committee of Regions but not when they are transferred to another institution. As for the data related to medical leave, these data are transferred to the new institution for the past three years. This is to ensure, as explained above, that the data remain available for an eventual invalidity procedure, which requires calculation of the number of days absent for medical reasons. Decisions on the granting of leave on personal grounds or family leave are filed in the personal file, but supporting data are not transferred.

Regarding security, as for the paper files, the rooms where the documents are stored are locked whenever they are unattended. The cupboards are also locked. Access to the computers is protected by individual passwords. For the IT systems the general horizontal security measures applicable to all EESC IT systems apply.

## 3. Legal aspects and Recommendations

**3.1. Applicability of the Regulation.** The notified management of medical leave, maternity leave and special leave falls under the scope of Regulation (EC) 45/2001 ("**Regulation**") pursuant to Articles 2 and 3.

**3.2. Grounds for prior checking.** The processing of data related to medical leave, maternity leave, and in certain cases, other types of leave (in particular, certain types of special leave) are subject to Article 27(2)(a) which requires prior checking by the EDPS of "processing of data relating to health". (We note that this Opinion also contains a couple of recommendations on related aspects of Centurio, which, in themselves, would not have been subject to prior checking.)

**3.3. Deadlines for notification and for issue of the EDPS opinion.** The processing was already in place at EESC before the EDPS was notified. The opinion of the EDPS should, as a rule, be requested and given prior to the start of any processing of personal data. Nevertheless, taking into account that a large number of processing operations were already in place before the EDPS started to operate in 2004 and some of the institutions and bodies have not yet fully cleared their backlog of notifications, these prior checking procedures are now carried out ex-post.

Pursuant to Article 27(4) of the Regulation, this Opinion must be delivered within two months, discounting any periods of suspension allowed for receipt of additional information requested by the EDPS. The procedure was suspended for 64 days. The Opinion must be provided no later than 9 March 2010.

**3.4. Lawfulness of the processing (Article 5(a) and Recital 27).** The management of absences and sick leaves is based on the Staff Regulations and the Conditions of Employment, as well as on formal internal implementing decisions as described in Section 2. Thus, specific legal instruments "adopted on the basis of the Treaties" allow and provide the basic conditions for the notified processing operations. The EDPS is also satisfied that the processing is necessary and proportionate for the management and functioning of EESC. Therefore, the processing is lawful.

**3.5. Data Quality (Articles 4(1)(a),(c) and (d)).** The EDPS has the following recommendations on data quality (adequacy, relevance, proportionality, fairness, lawfulness, or accuracy):

(i) **Access by management to detailed subcategories of data.** First and foremost, there is no reason why management (heads of units) should have routine access to the 60 or so detailed subcategories of data encoded by the competent department or by the medical service into Centurio. It is sufficient if the competent department or the medical service, as the case may be, has access to this level of detailed information, to verify and validate absences based on the supporting documents submitted by the staff member. For example, there is no reason why a manager would need to know whether an employee was on special leave because his/her spouse died, child became seriously ill or he/she was getting married. It is up to the employee to decide whether and in what way to share these often very personal details with his/her direct supervisor. Similarly, a head of unit does not need to have routine access to information on whether a medical leave that was authorized according to the Staff Regulation and the Conditions of Employment was certified or uncertified. It is sufficient if the competent department, or the medical service, as the case may be, verifies and validates such information. Therefore, any access to management should be limited, at most, to those 15 categories of data indicated on the list of presence that are first entered by each unit.

(ii) **Access by management to historic data.** Second, even if access is limited to the 15 categories on the list of presence, there is little or no added value in making available an individual's historic data for management. At the same time there is a risk to the privacy of the individual if his/her direct supervisor, by the push of a button, has access to intimate or personal details of his/her life, often dating back several years. For example, there is no reason why a head of unit should need to look up that an employee took three months off as a family leave ten years ago to care for a disabled or seriously ill relative, or took off two years fifteen years ago as leave on personal grounds. Neither should he/she need to be able to check, retroactively, whether an employee was or was not on strike last year. In addition to not being "necessary" in the first place, easy computerized access to historic data by management also leads to certain risks: some members of management may use the data for discriminatory purposes when making decisions such as the employee's annual evaluation, contract renewal, promotion, or assignment of tasks. This does not mean that management should have no access at all to any data in Centurio. Indeed, it is reasonable to have access to some *current* and *planned future* data for planning purposes. For example, it is reasonable for a head of unit to want to be able to check at any given time, whether a particular staff member whom he wants to give an urgent assignment to is on flexitime in the afternoon, has been off sick for three weeks, will be on mission tomorrow or has already introduced a plan to go on his/her annual vacation as of next week. The EDPS, in principle, has no objection against management access for planning purposes for current and future data, provided that the level of detail is not excessive (there are no unnecessary subcategories). Management can also have access to certain data for the past, with immediate effect on the present future. However, this should be clearly limited in time. While access to a couple of weeks or months back in time may be reasonable (e.g. as noted above, to see if a person has been on medical leave for over two or three weeks, which might suggest a serious or continued illness that may necessitate, for example, re-allocation of task), there is little justification for access for significantly longer periods back into the past.

(iii) **Access to the database by additional persons "in the interest of the service".** Fourth, currently it appears that it is fairly easy to obtain access to the database for additional persons. All that is required is permission from a head of unit that such access is "in the interest of the service". Indeed, in some units several employees take turn in inputting absence data in the database and they all have thus access to all data on the list of presence (although not to the detailed subcategories). In this respect, the EDPS recommends that EESC raises awareness among its management that access to Centurio should be limited on a strictly need-to-know basis. Among others, EESC should request those heads of units who currently arrange for data input on a rotational basis among their staff to reassess whether there is not a less intrusive alternative to input the data, without giving access to a large number of staff members' to each others' data. Second, the form on which access to Centurio is requested for a staff member should be redesigned to add, in addition to the words "in the interest of the service" also the requirement that access can only be granted in accordance with applicable data protection principles, in particular, with the principle of necessity and proportionality, on a strictly need-to-know basis.

(iv) **Access by medical service.** Fifth, access of the medical service to data in Centurio should be restricted to what is strictly necessary for well-defined objectives related to their mission. For example, it is reasonable that they should have access to current and future data on medical absences, including not only data on the list of presence but also on the detailed subcategories. Indeed, this is necessary to perform their job of verifying and validating medical absences in the database. However, there is no reason why the medical service should also have routine access to data on special leave or other types of absences. For example, it is hard to justify that the medical service would need to know whether an employee was on strike or at an EPSO exam at any time. If there is a specific need for access to any specific data, this may be accommodated, but the necessity of access must be clearly demonstrated. General claims to eventual utility such as that "information on recent requests for special leave for the illness of a loved one may assist the Medical Service staff in their 'global treatment' of a staff member" are insufficient. Further, the fact that medical staff are bound by a duty of confidentiality does not mean that they can have access to personal data that are irrelevant to their work (such as strike data) or to data that can be obtained by other means when needed (such as during a personal discussion at the annual exam if it appears that the illness of a loved one necessitates some form of preventive action by the medical services). As for historic data, the necessity of access to this should also be justified (for example, some data may be necessary for the case of an eventual invalidity assessment) or access must be reconsidered.

(v) **Staff directory: "absence from the office".** Sixth, the EESC should remove the indication from its staff directory whether a particular person is "absent from the office" on the particular day when the database is consulted. This information has limited utility. At the same time, it unnecessarily allows employees to monitor each others' presence at the office throughout the organization. In this respect we emphasize that the EESC employs over 800 employees, many of who do not know each other personally and do not routinely need to know whether any particular person outside their own teams is absent or present on a particular day. Alternative, less intrusive methods can be used to find out whether an employee is absent or present. To start with, an email or telephone call can be made to try to reach the employee. If the employee cannot be reached momentarily, in most well-

organized units, it is fairly easy to find out if any particular person is in or out of the office and when he or she will be back. For example, out-of-office replies and answering machines can provide details of whom to contact in case of absence. The secretariat/assistant of the head of unit, or another team member can also often help. He or she will usually be able to provide more detailed information, in any event, then the information noted in Centurio. Further, if a more immediate ability to contact each other is needed for certain individuals or groups of people, this can be done on a voluntary basis. For example, team members (e.g. members of the same unit) may voluntarily share outlook calendars with each other. This is also possible across teams within the larger organization, or on a temporary basis. If desirable, the current application in the Centurio directory may also be configured to allow seeing whether someone is in or out based on the employee's specific, informed and freely given consent only.

(vi) **Staff directory: temporary contracts.** Seventh, there is no reason for the directory to make it publicly available knowledge within the institution whether a staff member is on a temporary contract or an official. This is information that many staff members consider highly personal. If anyone has a legitimate interest for knowing this information, this can be shared on a case by case basis, without routine access through the intranet.

(vii) **Staff directory: photos.** Eighth, while photos are a useful addition to the staff directory which many people like to use, they are by no means strictly "necessary." Some individuals are also uncomfortable with it. Therefore, it must be made clear that they are uploaded only based on clear and informed consent. This can be given, for example, at the time when the photo is taken for the badge, by ticking off a specific box on the form that is completed at this time. Ideally, staff members should also have a say what photo is uploaded and should be able to opt for a different photo than the one on their access badges.

### 3.6. Retention of data (Article (4)(1)(e)).

The EDPS welcomes that clear retention periods are set forth for different types of absences and that these apply to both on-line data and hard-copies or supporting documents.

As for medical leave, the EDPS accepts the proportionality of a retention period slightly exceeding the three years that would be strictly required[4], for the practical reasons explained by EESC in connection with the annual deletion cycle in January-February. However, to further improve the procedures, the EDPS recommends that

- the retention period should be reduced to a maximum of four years rather than five years;
- the EESC should ensure also that also the medical certificates that are held by medical service are destroyed at the same time as online data.

[4] See, for example, the EDPS Guidelines of health data at work: Guidelines concerning the processing of health data in the workplace by Community institutions and bodies, 28 September 2009, page 12, Section 4 of the Data related to sick leave: "Article 59 (4) of the Staff Regulations could justify a conservation period of 3 years for data necessary to justify an absence due to sick leave. The only justification for keeping them any longer would be if a dispute or appeal were under way."

As for special leave and all other absence data (except for medical leave, family leave and leave on personal ground, which each requires specific data retention periods already specifically addressed), the EESC should reassess whether they should be indeed kept for a period of a maximum of five years, as currently done. For most categories of leave, a shorter period not exceeding one or two years will likely be sufficient and appropriate. When establishing retention periods, special attention should be paid to data that are potentially sensitive, such as whether an employee was on strike.

Finally, it must be verified that the retention periods are made automatic and incorporated into the system architecture of the Centurio database. As a good practice, we also recommend EESC, which developed Centurio, and made it available for other EU bodies for use, to call other users' attention to this opinion, and, if possible, offer them to incorporate similar changes into their systems.

**3.7. Right of access and rectification (Article 13).** The EDPS welcomes the direct read-only access of staff members to the application as well as the annual verification process. The EDPS also welcomes the informal procedures in place to allow rectification in a timely and effective manner.

**3.8. Information to the data subject (Articles 11 and 12).** Articles 11 and 12 of the Regulation require that certain information be given to data subjects in order to ensure the transparency of the processing of personal data. The EDPS welcomes that EESC provides a layered notice to staff members and uses a combination of methods to provide comprehensive information: formal internal decisions, formal data protection notices on the intranet at an easily available location near to the information on the particular types of leaves, and on the forms themselves.

**3.9. Security measures (Article 22).** The EDPS has no specific recommendations on the technical and organisational measures taken by the controller to protect the data. Nevertheless, the EDPS highlights the fact that EESC should ensure that data are not accessible by or disclosed to anyone other than those specified in Section 2.

**Conclusion**

The EDPS finds no reason to believe that there is a breach of the provisions of the Regulation provided that the recommendations in Section 3 are implemented, namely:

- **Retention of data**
    - EESC should slightly shorten the retention period for medical leave (to four from five years).
    - EESC should also reconsider the retention period, on a case by case basis, for each other type of leave for which the retention period is currently also set at five years. In most cases, a retention period not exceeding one or two years may be appropriate.

- **Proportionality**
    - EESC should reconsider the rules governing who has access to what data and for what period of time.

- In particular, access to management should be limited to a lesser set of categories and for a shorter period of time, not including historic data.
- Access to assistants and others upon authorization by the heads of units should also be more limited.
- Medical service should only have access to medical leave data and not to other types of leave data. Their access to historic data should be reconsidered.
- In the staff directory, which is available for all for viewing on the EESC intranet, there is no need to indicate whether an individual is on a temporary contract or a permanent official and whether he is in or out of the office on a particular day. Photos should be uploaded only based on clear opt-in consent.

Done at Brussels, on 5 March 2010

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor