Opinion on the notifications for prior checking from the Data Protection Officer of the European Railway Agency (ERA) regarding ERA's e-mail system and back-end e-mail system

Brussels, 6 December 2012 (cases 2012-136 and 137)

1. PROCEEDINGS

On 10 February 2012, the European Data Protection Supervisor ("**EDPS**") received from the Data Protection Officer ("**DPO**") of the European Railway Agency ("**ERA**" or the "**Agency"**) two notifications for prior checking relating to, respectively, ERA's e-mail system and ERA's back-end e-mail system. Before filing the notifications, ERA consulted the EDPS on the need for prior checking pursuant to Article 27(3) of Regulation EC 45/2001 (hereinafter the "**Regulation**"). The notifications were accompanied by the following draft-documents:

- Policy 2.0 Use of ERA ICT[1] Owned Resources ("**ICT**")
- Policy 2.1 Identity and Access Management ("**IAM**")
- Policy 2.2 Internet Acceptable Use Policy ("**Internet Policy**")
- Policy 2.3 Electronic Communication Policy ("**ECP**")
- Policy 2.4 E-mail Acceptable Use ("**E-mail Policy**")
- Policy 2.5 Electronic Information Security Policy ("**EISP**").

The back-end part of the e-mail system is the part that concerns the communication between the email servers (e.g. Microsoft Exchange) and the external world/internal users (as opposed to the client-end part, which is the software used by the users to access their email, e.g. Microsoft Outlook, a browser for web email, etc). Since there is no clear difference between the two notifications, the EDPS will deal with them jointly. The present Opinion refers to both notifications jointly as "E-mail Policy".

The EDPS requested ERA to provide some complementary information on 2 April, 2 July, 7 and 28 September and 26 October 2012. The answers were received on 4 May, 5 and 25 September, 15 and 17 October and 15 November 2012.[2] On 10 May 2012, the EDPS decided to extend the time limit for issuing an Opinion by two months, in accordance with Article 27(4) of the Regulation, because of the complexity of the matter. A meeting between EDPS and ERA services took place on 10 October 2012 in order to clarify some points.

[1] Information and Communication Technology.
[2] The complete answers for all the questions asked on 2 July and on 7 September 2012 were not received until 17 October 2012. The EDPS considered therefore the period between 2 July and 17 October as a continued suspension.

2. FACTS

The present prior-check Opinion concerns ERA's policy on e-mail system and back-end e-mail system, as described in the E-mail Policy and the ECP. The organisational part of the institution or body entrusted with the processing is the Administration Unit.

In addition to these specific notifications, ERA sent as background documents to the EDPS its written policies concerning ICT, IAM and EISP. While these documents do not technically fall within the subject-matter of the present Opinion, the EDPS will refer to them insofar as relevant.

2.1. Purposes of the processing

The purposes of the E-mail Policy declared by ERA are the following:

- outline appropriate and inappropriate use of the e-mail system;
- ensure that the Agency's e-mail systems are used for purposes appropriate to the Agency's mission;
- inform the Agency's community about the applicability of rules and ERA's policies with regard to e-mails;
- prevent disruptions and misuse of the e-mail systems and services.

2.2. Categories of data subjects

The notifications describes the categories of data subjects involved as follows:

- anybody whose e-mail address appears in the "To", "From", "CC", and/or "BCC" traffic fields of an e-mail message, as soon as these messages have been processed by the e-mail servers of ERA;
- regarding the management of the e-mail address book, all staff of European institutions/agencies and bodies with whom a convention relating to Article 7 of Regulation 45/2001 (Transfer of Data") has been established and signed;
- ERA statutory staff members, officials and statutory staff members from other European institutions/agencies/bodies, "Seconded National Experts", trainees and subcontractors;
- European and third country citizens.

2.3. Allowed and prohibited use

According to ERA, e-mail services should not be used for purposes that could reasonably be expected to cause excessive strain on any electronic communication resources, or to cause interference with others' use of electronic resources. In that context, e-mail users shall not in particular:

- send or forward chain letters or their equivalents in other services;
- "spam", that is, exploit electronic communications systems for purposes going beyond their intended scope to amplify the widespread distribution of unsolicited electronic messages;

- "letter-bomb", that is, to send an extremely large message or send multiple electronic messages to one or more recipients and so interfere with the recipients' use of electronic communications systems and services;
- intentionally engage in other practices such as "denial of service attacks" that impede the availability of electronic communications services.

Incidental personal use is allowed as long as it does not (i) interfere with the Agency's operation of electronic communications resources; (ii) interfere with the user's employment or other obligations to the Agency, or; (iii) burden the Agency with noticeable incremental costs.

2.4. Monitoring of use

The E-mail policy specifies that spam and viruses are automatically filtered before reaching the users. Furthermore, the ICT policy informs the users that the Agency will routinely monitor usage patterns of the ICT resources and states that this is done to ensure the functionality of the ERA information systems and avoid security breaches. The ICT policy also states that the content of communications will not be subject to any monitoring.

ERA's e-mail users should not use the e-mail services to transfer certain data, such as user names, passwords, social security numbers and account numbers over the Internet. Users should not use the e-mail system to transfer sensitive data, except in accordance with ERA's data protection policies.

2.5 Access to e-mails without consent

Section IV of the document outlines the rules concerning requests to examine e-mail without the user's consent. The document states that ERA does not need in general consent to examine files stored on an individual's computer as these files do not meet the ECP definition of an "electronic communication record". When reviewing such files, however, colleagues have an obligation to respect confidentiality of personal communications. Any review should be limited to the minimum necessary.

In order to access a job holder's e-mail, ERA considers as necessary to ask for the consent of the account holder in line with the rules outlined in Section V of the ECP. Non-consensual access can be requested only in "*very limited circumstances*", as described in the ECP and the E-mail Policy (Section IV B):

- the staff member no longer works at ERA or is deceased. In this case, access is permitted normally without filing a formal request for non-consensual access;
- staff-members on leave. The Head of Unit/Sector or direct superior (the "requestor") should ask a staff-member in advance for permission to access his or her e-mail during the period of leave to ensure business continuity if necessary. This permission can also be requested from the staff-member while he/she is on leave. If this is not possible, the requestor should follow the ECP procedures for obtaining non-consensual access.
- criminal investigations or sensitive matters: This scenario covers situations where: (i) the staff-member cannot or does not want give consent, (ii) the staff-member must not be alerted, (iii) a criminal investigation is ongoing regarding a former post-holder. In this case, the requestor must contact ERA Security Officer who should follow the procedures for obtaining non-consensual access.

If individuals wish to obtain access without the person's consent, they must complete a specific form called "Non-consensual Access Form" (except in cases falling under the first bullet point above).

The procedure to be followed for obtaining non-consensual access is further described in the ECP. Access to electronic communications must be authorised by the Executive Director, or the Head of the Administration, or other delegated function, in consultation with ERA Data Protection Officer and ERA IT Security Officer. ERA should always seek the advice of ERA's DPO and/or ERA's legal services before accessing without consent electronic communications records (see ECP, p. 14).

The authorisation shall be limited to the least perusal of contents and the least action necessary to resolve the situation. In emergency situations, the ECP allows for immediate access to be performed without authorisation and with appropriate safeguards. Authorisation should be asked without delay.

2.6. Categories of personal data

The categories of data involved are:

- for the e-mail message, the message header (traffic information) - subject, body of the message (i.e. its content) and attachments;
- for the address book: first name, last name, alias (information login), office phone, unit or sector, e-mail address.

2.7. Data transfers/recipients

As regards e-mails, recipients are potentially anybody in the world who has an e-mail address, including EU institutions', agencies' and bodies' staff members. As to the Address Book, recipients would include staff of ERA, e-mail services of the EU institutions, staff of the EU agencies and bodies with which ERA concluded a bilateral agreement.

2.8. Conservation of data

The personal data in e-mails are kept for as long as the data subject has an active e-mail account and until 90 days after its deactivation or 13 months after the deletion of the e-mail account in logs and backup media. The personal data in address books are kept for as long as the data subject is employed with ERA.

2.9. Rights of the data subjects

Data subjects will be informed by means of a Note to the Staff "Use of ERA's ICT owned resources", the ICT, the IAM, the ECP and the E-mail Policy.

When a staff member takes up his duties he/she is informed of the Regulation safeguarding, amongst others, the rights to access and rectification of data subjects and to require ERA to rectify without delay any data which is inaccurate or incomplete or to erase data when processing is unlawful. Data subjects can exercise their rights by contacting ERA by e-mail. ERA shall deal with the requests for rectification in one month from the introduction of the request. Requests for blocking and erasure have to be answered in three months. The data subjects can address at any time the DPO by e-mail.

2.10. Security measures

Several system specific security measures are implemented and described in the E-mail policy:

- the system is integrated within the IAM system implemented at the Agency. Users are informed that they should not communicate their password, even to the Service Desk;
- in order to combat viruses, certain attachments types may be stripped at the corporate e-mail gateway. Recipients are notified by e-mail when this occurs. As attachments can contain viruses and other malware, users are informed that they should only open attachments from a trustworthy source and suspicious items should be forwarded to the Service Desk;
- spam is automatically filtered at the corporate gateway. E-mails identified as clear spam are deleted on the basis of a domain blacklist before receiving them at the e-mail gateway. Suspicious e-mails are put in local junk e-mail folder;
- access to log files is reserved to administrators of the e-mail system (daily operations), and other competent authorities (e.g. OLAF).

Additional measures covering all systems are described in the EISP and include:

- the need for risk management and the need to determine cost-effective controls to prevent against these risks;
- a description of the roles and responsibilities also covering security aspects;
- rules for classified information;
- a list of the necessary security procedure that need to be defined;
- operational and technical controls (backups, patch and change management processes...);
- the need to provide training and security awareness.

3. Legal aspects

3.1. Prior checking

This prior checking Opinion relates to ERA's policies concerning e-mail use, including data processing actions directed at monitoring users' behaviour. Accordingly, the Opinion assesses the extent to which the data processing operations described above carried out by the relevant ERA's actors are in line with the Regulation.

3.1.1. Applicability of the Regulation

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

First, the monitoring of the use of the e-mail entails the collection and further processing of *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001. This includes e-mail traffic records detailing the way the e-mail is used by individual ERA staff members (transactional data) as well as the content of the e-mail messages.

Second, as described in the notifications, the personal data collected undergo *"automatic processing"* operations, as defined under Article 2(b) of the Regulation as well as manual data processing operations. Indeed, the personal information is first collected automatically

(automatic registering of log files) and automatically handled by the system (spam and virus filtering) and may then be subject to analysis by the relevant IT staff.

Finally, the processing is carried out by an EU institution, in this case by the European Railway Agency, in the framework of EU law (Article 3(1) of the Regulation). Therefore, all the elements triggering the application of the Regulation are present.

3.1.2. Grounds for prior checking

Article 27(1) of the Regulation subjects to prior checking by the EDPS *"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"*. Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks. This list includes, under paragraph (a) "*processing of data relating to health and to suspected offences, offences...*" and (b) "*processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency or conduct*".

Taking into account on the one hand that the monitoring of the use of the e-mail as described in the submitted policy documents may lead to the evaluation of users' conduct (to assess whether or not their use is in line with ERA's E-mail Policy) and, on the other hand, that such monitoring may entail the collection of data related to suspected offences (if there is a suspicion of unlawful behaviour) as well as other types of sensitive data, such monitoring and related data processing operations must be subject to prior checking *ex* Article 27 (a) and (b) of the Regulation.

The prior checking pursuant to Article 27 of the Regulation should in principle take place before the processing has initiated. The EDPS therefore deeply regrets in the present case that the notifications were not submitted to him prior to the start of the processing operations.

3.1.3. Notification and due date for the EDPS Opinion

The notifications were received on 10 February 2012. The period within which the EDPS must deliver an opinion pursuant to Article 27(4) of the Regulation was suspended for 178 days to obtain some complementary information.

Moreover, on 10 May 2012, the EDPS extended the time limit by two additional months in view of the complexity and sensitivity of the matters involved and the parallel development by the EDPS of horizontal guidelines on the subject of e-monitoring.

The Opinion must therefore be adopted no later than 6 December 2012.

3.2. Lawfulness of processing

Personal data may only be processed if legal grounds can be found in Article 5 of the Regulation. The notifications justify the processing operations on the basis of Article 5(a) of the Regulation, i.e. processing necessary to perform a task in the public interest. Furthermore, the E-mail Policy refers in various circumstances to the consent of the data subject (Article 5(d) of the Regulation). This legal basis will be analysed in more details below (sub-sections 3.2.1 and 3.2.2.).

In addition, the EDPS will focus on some specific processing activities described in the ECP and E-mail Policy which raise specific concerns from the point of view of lawfulness (sub-

sections 3.2.3-3.2.6).

3.2.1. Article 5(a) – processing necessary to perform a task in the public interest

Article 5(a) foresees that 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*".

In order to determine whether the processing operations comply with Article 5(a) of the Regulation two elements must be taken into account: first, whether either the Treaty or other legal instruments foresee a task carried out in the public interest on the basis of which the data processing takes place (*legal basis*), and second, whether the processing operations are indeed necessary for the performance of that task, i.e. necessary to achieve the intended goals (*necessity*).

- Legal basis

First, the EDPS notes that the Regulation contains various provisions that are relevant to evaluate the lawfulness of the monitoring of e-mail usage by ERA. In particular, Recital 30 of the Regulation establishes that "*[i]t may be necessary to monitor the computer networks operated under the control of Community institutions and bodies for the purposes of prevention of unauthorised use*". As outlined above, one of the purposes sought by ERA when it engages in monitoring of the e-mail is to prevent that this instrument is used in violation of law, ERA's internal policies or in a way that is otherwise not authorised.

Moreover, Article 37(2) of the Regulation provides for an additional legal ground authorising ERA to carry out a very specific data processing activity, i.e. to keep traffic data, in this case, log files. In particular, Article 37 (2) provides that traffic data may be processed for the purpose of telecommunications budget and traffic management, including the verification of the authorised use of the telecommunications systems. The concept of "*verification of authorised use*" is key as it concerns the possible use of traffic data beyond traffic and budget management. In particular, it allows the use of traffic data to ensure the security of the system/data and respect of the Staff Regulations or other provisions such as those included in the E-mail Policy.

Additionally, the EDPS considers that ERA in its role as employer has certain duties and is bound by certain obligations deriving from employment law that can be considered as appropriate legal grounds to justify a proportionate processing. For example, ERA's duty to protect itself from liability linked to workers' actions may also justify the processing. This may include the processing of special categories of data, in certain circumstances (see Section 3.3).

Finally, the policy documents issued by ERA constitute another element in determining whether there is an adequate legal basis for the purpose of Article 5(a) of the Regulation, as they set forth rules concerning the monitoring of electronic resources for, among others, ensuring security and the verification of authorised use.

- Necessity

As described above, one of the main purposes of the processing under evaluation is to ensure that the Agency's e-mail systems are used for purposes appropriate to the Agency's mission, as laid down in the E-mail Policy, and prevent disruptions and misuse of the e-mail systems and services. The EDPS takes note that ERA considers as necessary to engage in some monitoring

of the use of its e-mail systems, with a view to being able to prevent or detect violations of its e-mail policy or security breaches. Therefore, it appears that a selective and lawful monitoring of e-mail systems may be, at least to some extent, considered as necessary for the purpose of carrying out the task of ensuring a use in accordance with the E-mail Policy and thus, for ensuring the overall security of ERA's ICT resources.

Some monitoring is also considered as necessary by ERA for the purposes of enabling it to exercise, where appropriate, its rights and obligations derived from employment law. For example, ERA declares that if it would not be able to monitor the use of an individual suspected of engaging in behaviour against its policy (for example, leaking confidential documents) it may not have the necessary evidence to open disciplinary proceedings.

In the light of the above, the EDPS takes note that the notified processing can be considered as necessary for achieving the intended purposes of the policy. The requirements for compliance with Article 5 (a) of the Regulation seems thus to be satisfied in principle. In monitoring the use of e-mail, ERA should always respect necessity and proportionality in line with the data quality principle, as discussed in Section 3.4.

3.2.2. Article 5(d) – consent of the data subject

The ECP states that in principle ERA examines electronic communications data only with the user's consent. For consent to be valid, it must be freely given, specific and informed. The user shall be aware of the processing operations particularly for those based on his/her consent, also with regard to certain essential details thereof, including the consequences of his/her choices.

The use of consent faces specific limitations in situations where the data subject finds himself in a situation of dependence or weakness vis-à-vis the data controller. This is the case in particular with regard to employment relationships.[3] The EDPS considers that consent may be used as a valid ground for processing personal electronic communications data in an employment relationship only in limited and exceptional cases.

3.2.2.1. Access to e-mails in the absence of the user

One case where consent could be exceptionally used to obtain access to electronic communications is when access relates to business continuity purposes, i.e. when the user is absent or no longer working and the employer needs access to professional e-mails.[4] Although, as said, consent is not the ideal pre-requisite for such a processing of personal data, the "agreement" of the data subject helps in reducing tensions at the workplace.

With regard to this event, the user should be provided with all the necessary information, notably on the reasons for demanding access, the urgency of the matter, the nature and scope of information sought and the other information listed in Article 11 of the Regulation. ERA has submitted to the EDPS a Consent Form to be used in these cases. The Form contains fields concerning (i) the reasons for granting access, (ii) the scope of access, (iii) the period of access, and (iv) proportionality and confidentiality obligations to be respected. The EDPS has the following comments regarding the content of the form:

- the Form should specify in a clear and conspicuous manner that consent is free and revocable at any time and that the user will not suffer any adverse consequences in case he/she refuses;

[3] See, e.g., Article 29 Working Party Opinion on the definition of consent, 13 July 2011 (WP187), p. 13 et seq.
[4] See Opinion of 18 January 2010–Court of Auditors procedure to access private drive e-mail (C 2009-0620).

- the expression "all records necessary to conduct Agency business" is too wide. The EDPS recommends replacing this formula with a more precise definition;
- the following information under Article 11 should be included: the identity of the controller; the recipients or categories of recipients; the existence of the right to access to any e-mail received and sent through the account in the intervening period.

It would only be in the case of the impossibility to obtain the user's consent (if the user is not reachable or not in the capacity to consent), or the impossibility to implement alternative organisational or technical solutions (e.g. functional mailboxes, see below) that Article 5(a) should be considered as the legal basis. The EDPS is of the view that the access in the context of the procedure could only be considered as necessary towards achieving the intended purposes if ERA can demonstrate that the staff member received a clear and complete information regarding the use of private/professional e-mail and private drive, that the matter of urgency of the access requested could be demonstrated and that the consent of the user could not be received. These aspects of the necessity would need to be demonstrated on a case by case basis. In addition, whenever access is performed in the absence of the user, the latter must be individually informed.

It is also important to underline that such procedure of access shall not be considered as part of an administrative inquiry procedure against a staff member. To be more precise, this procedure shall not serve as a way to circumvent the rules established in the case of an administrative enquiry procedure or disciplinary procedure against a staff member. The DPO of the ERA should demonstrate, in his written opinion, that she analysed this aspect.

In addition or as an alternative to the above methodology, ERA may consider introducing common mailboxes and request recipients to copy business related correspondence to this mailboxes. In that case, access to the common mailboxes may be granted in principle to all members of the unit. This approach would reduce significantly the need to have access to individual e-mails for business continuity purposes.

Concerning the e-mail account of users no longer working for the Agency, before their departure the staff should be requested to empty his/her e-mail account of its private content. In order to deal pro-actively with access requests by former staff members, the EDPS considers it would be good practice to provide a copy of the content of the private e-mails, which have been designated as such by the user (or of the private drive containing such e-mails) in a CD/DVD format.

Section IV B of the E-mail Policy (as described in Section 2.5 above) and related sections of the ECP should be amended/reconsidered in order to conform to the above recommendations.

3.2.2.2. Access of files stored in individual's computer

The E-mail Policy states that "*when reviewing files on an individual's computer, consent to access generally is not required because those files do not meet the ECP definition of "an electronic communication record*"". The EDPS does not share this statement as the definition of "electronic communication record" according to the ECP is "*The content of electronic communications created, sent, forwarded, replied to, transmitted, distributed, broadcast,* ***stored****,* ***held, copied, downloaded,*** *displayed, viewed, read, or printed by one or several electronic communications systems or services*" (emphasis added). The files stored in a user's computer may thus well contain personal data, including e-mails. The EDPS takes the view that files stored in individuals' computers should be subject to the same rules concerning access to e-mails in the absence of a user.

The EDPS therefore recommends that ERA extends to this type of access the same rules foreseen for access to e-mail in the absence of a user (see Section 3.2.2.1. above).

3.2.3. Personal webmail accounts

The E-mail policy states that "*it applies to post-holder use of personal e-mail accounts via browsers, as directed below*". In further exchanges with the EDPS, ERA specified that "*any ERA post-holder, using ERA ICT infrastructure, may use a private e-mail account. Although this e-mail account is external to the ERA IT system, when using it through internet connection, it will appear that the access is made by the Agency IP addresses. In this respect, it is expected that the users behave in compliance of the policy terms*".

Generally speaking, the employer cannot regulate or influence the use by the employees of their personal webmail accounts, even if the latter are accessed by means of Agency connections. Personal webmail accounts fall generally outside the remit of the controller sphere of influence; they belong to the private domain and thus the employer has no right in principle to interfere. The fact that use of personal account at work will appear to be made by the Agency IP addresses does not seem to constitute a plausible justification for subjecting personal webmail account to ERA's E-mail Policy. This is further demonstrated by the sheer incompatibility with certain provisions thereof, such as those regarding e-mail account activation/deactivations, restrictions, incidental personal use, access without consent, etc.

There could be some exceptions to this general rule, such as prohibitions to download files or even to access personal e-mail accounts insofar as they are justified and proportionate. The E-mail Policy does not provide, however, any detail concerning the specific situations as to when the E-mail policy would apply to the use of personal webmail accounts. General application of this policy to personal webmail accounts cannot be maintained.

On similar grounds, the EDPS finds over-intrusive and restrictive the provision of the ECP stating that "*ERA post-holders are prohibited from seeking out, using, or disclosing personal information in electronic communications without authorisation*". The scope of this provision is too wide. It implies that ERA users are not allowed to use e-mails for personal use or for professional messages containing personal data. The first reading would be in contrast with the fact that the ECP allows incidental personal use, while the second would appear unrealistic.

The EDPS therefore calls ERA to reconsider the above provisions and redraft the related parts of the E-mail policy to take into account the above considerations.

3.2.4. Access to public records

The ECP contains a specific definition of "Agency Electronic Communication Record" ("ECR"). This is defined as follows:

"*[e]lectronic communications records pertaining to the administrative business of the Agency are considered public records,* ***whether or not the Agency owns the electronic communications resources systems or devices used*** *to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, print, or otherwise record them.* ***Other records, although not owned by the Agency****, nevertheless may be subject to disclosure as public records under EU legislation if they pertain to the business of the Agency*" (emphasis added).

The above definition of Agency's ECRs presents evident links with the notion of public document for the purpose of Regulation 1049/2001 on public access to documents. The fact that Agency's ECRs are considered as public records may indeed imply an obligation to grant access to those records under the above Regulation. However, the definition provided appears to go beyond the EU definition of "public document". In this regard, the EDPS highlights that in order to be applicable Regulation 1049/2001 requires that the document has to be a document "*held by an institution*", that is to say *"documents drawn up or received by it and in its possession, in all areas of activity of the European Union*". The EDPS invites therefore ERA to reflect upon such definition to ensure that it remains consistent with the above-mentioned Regulation.

The ECP also states that "*any electronic communications record residing on Agency-owned or controlled communications, video, audio, and computing facilities will be deemed to be an Agency electronic communications records for the purposes of this Policy. This would include personal electronic communications*" (emphasis supplied). While the meaning of the last sentence is not entirely clear, the EDPS has to underline the potential inconsistency in the above cited passage stemming from the idea that personal electronic communications might be subject to public disclosure. As long as they are truly personal (not related to the performance of the Agency's tasks), personal communications fall outside the scope of application of Regulation 1049/2001. The EDPS therefore recommends that ERA reconsiders and/or clarify the passage in question.

3.2.6. Interception of telephone conversations

The ECP provides that "*audio or video telephone conversations shall not be recorded or monitored without advising the participants unless a court has explicitly approved such monitoring or recording*".

In light of the case law of the European Court of Human Rights, the EDPS considers that interception of electronic communications may take place only in presence of a sufficiently precise and specific legal basis.[5] In particular, the interception must be clearly authorised by law and based on a specific legal instrument defining the circumstances in which and the conditions under which the interception can be carried out, as well as providing appropriate safeguards against the risk of abuse. An administrative act cannot in general be considered sufficient in this regard.

The EDPS is not aware of any legal instrument authorising in the sense outlined above the interception of electronic communications by ERA. The general legal bases for administrative investigations and disciplinary proceedings do not normally qualify as sufficient legal basis for telephone interceptions. Quite to the contrary, according to Recital 19 of the Regulation, ERA should ***inform*** the competent authorities in the Member States when they consider that communications on their telecommunications network should be intercepted in keeping with national laws but is not entitled to perform the interceptions by itself.

In the EDPS view, therefore, ERA lacks a sufficiently precise and specific legal basis in order to carry out interceptions of electronic communications at the workplace. He recommends that ERA removes the above cited passage from the ECP.

3.3. Processing of special categories of data

[5] See, e.g., ECtHR, *Kruslin v. France* (11801/85) judgment of 24 April 1990, paragraph 33; ECtHR, *Malone*, cited above, paragraph 68.

The monitoring of the e-mail use may reveal special categories of personal data. These data are qualified by the Regulation as any personal data "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life*" (Article 10). Especially the content of some e-mails may reveal very intimate details of one's personal life, such as sexual preferences, health data or political orientations. Even the processing of traffic data, such as e-mail log files, may sometimes qualify as special category of data, such as in cases where e-mails are sent to "sensitive recipients" such a trade union, a political party and similar organisations.

The processing of special categories of data is in principle prohibited unless one of the exceptions laid down in under Article 10 of the Regulation applies. Article 10(2)(b) of the Regulation establishes that the prohibition shall not apply where the processing is "*necessary for the purpose 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*". Some monitoring of the e-mail usage may be deemed necessary for ERA to ensure the security of the system/data, as well as compliance with the Staff Regulations and other provisions.

This would comprise, for example, ERA's right to prevent the viewing or exchanging of sex related contents or information in the workplace. Monitoring of sensitive information may also be justified in certain cases in order to enable the employer to exercise his rights as employer such as his right to initiate disciplinary proceedings including for the dismissal of employees who engage in unlawful activities such as viewing and downloading materials that promote crime. Therefore, the EDPS considers that ERA, as an employer, is subject to rights and obligations derived from employment law that may justify the processing of sensitive data of users which is necessary and proportionate in the context of internal investigations.

Having regard to the processing of personal data in the framework of administrative investigations, the EDPS refers ERA to the guidelines on administrative inquiries and disciplinary proceedings.[6]

3.4. Data quality

3.4.1. 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. This is referred to as the data quality principle.

The stated purpose of ERA's E-mail Policy is to:

- outline appropriate and inappropriate use of the e-mail;
- ensure that Agency's e-mail systems are used for purposes appropriate to the Agency's mission;
- inform the Agency's community about the applicability of rules and ERA's policies with regard to e-mails;
- prevent disruptions and misuse of the e-mail systems and services.

As described above, e-mail processing for security purposes consists essentially in the systematic automated inspection of e-mail messages going through an institution's

[6] Guidelines concerning the processing of personal data in administrative inquiries and disciplinary proceedings by European institutions and bodies, 23 April 2010, available on EDPS website.

telecommunications network for the purpose of eliminating viruses or other malware as well as spam. As it is performed by automated means, this process does not normally imply the manual processing of personal data. The EDPS has no particular comment on this approach, which corresponds to the standard practice in these cases.

Having said this, he points out that the individual examination of electronic communication data relating to e-mail, including content, can only be performed in presence of an adequate suspicion of wrongdoing which is corroborated by concrete initial evidence and in the framework of an administrative investigation. Access should be proportionate and not go beyond what is appropriate and proportionate having regard to the specific circumstances. A clear procedure should be set up in this regard based on a gradual and proportionate approach. Having regard to the processing of personal data in the framework of administrative investigations, the EDPS refers ERA to the guidelines on administrative inquiries and disciplinary proceedings.[7]

The ECP refers to the following circumstances where access without consent is allowed: 1) when is required and consistent with law; 2) when there is substantiated reason to believe that violations of law or of the Agency policy have taken place; 3) when there are "compelling circumstances" as defined in the Annex; 4) under "time dependent, critical operational circumstances" as defined in the Annex. It further states that except in "emergency circumstances", such actions must be authorised in advance and in writing by the Executive Director, or the Head of Administration, or other delegated function, in consultation with ERA's Data Protection officer and ERA's IT Security Officer.

The EDPS welcomes the fact that the DPO is consulted before access to e-mail is performed without consent. However, he would point out that terms such as "compelling circumstances", "time dependent, critical operational circumstances" and "emergency circumstances", albeit defined, are too general and overlapping. He therefore recommends that ERA reconsiders the use of such terms in its policies. In particular, ERA should further specify and clarify the said definitions.

3.4.2. Fairness and lawfulness

Article 4(1)(a) of the Regulation requires that data 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 which is further addressed in Section 3.8.

3.4.3. 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"*. ERA must take every reasonable step to ensure that data are up to date and relevant. In this respect, see also Section 3.8.

3.5. Conservation of data

Pursuant to Article 4(1)(e) of the Regulation, personal data may be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which

[7] Cited above.

the data are collected and/or further processed.

According to the notifications and the E-mail Policy, data are retained as long as the data subject has an active e-mail account until 90 days after the de-activation of the e-mail account and 13 months after the deletion of the e-mail account, in logs and back-up media.

This timing is not completely in line with Article 37 of the Regulation which provides for specific measures as concerns the conservation of traffic and billing data. Article 37.2 of the Regulation indeed provides that traffic data must be erased or made anonymous as soon as possible and in any case no longer than six months after collection, unless they need to be kept for a longer period to establish, exercise or defend a right in a legal claim pending before the court. ERA may therefore decide to keep the logs for a maximum period of 6 months.

If monitoring of log files or traffic data leads ERA to suspect that an individual has infringed the E-mail Policy, ERA will be allowed to keep the incriminating log files in order to "*establish, exercise or defend a right in a legal claim pending before the court*". In this context Article 20 of the Regulation is also relevant insofar as it provides for possible restrictions to the principle of immediate erasure of the data as established in Article 37.1, notably when the restriction constitutes a necessary measure to safeguard "*the prevention, investigation, detection and prosecution of criminal offences"*. The EDPS has interpreted this provision as covering not only criminal investigations, but also disciplinary proceedings.[8]

Thus, where relevant, log files may be processed in the framework of an administrative inquiry, whether it be a criminal or disciplinary offence. It should be noted that this measure should only take place on a case by case basis, when there is a legitimate suspicion that an individual has infringed the E-mail Policy, the Staff Regulations or committed a criminal offence and ERA has opened an administrative inquiry. At the end of the first six months an assessment is required to judge whether the data collected and verification carried out are such as to reasonably support the continuation of the investigation (which should be officially opened) or the launch of a disciplinary proceeding. Only in cases where this assessment leads to a positive outcome, can traffic data be retained longer than six months; it should be noted that in these cases, only the relevant parts of the logs files should be kept.

3.6. Transfers of data

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

According to the notifications the data may be accessed internally only by the IT Security Officer and the Head of IT. In further exchanges with the EDPS, ERA added the following internal recipients, specifying that they personal data could be transferred to them within the "Incident management process" (technical incidents, security incidents), i.e. whenever there is an incident severe enough to be escalated to this level of hierarchy:

- Executive Director,
- Data Protection Officer,
- Head of Administration Unit,
- Concerned Head Unit,

[8] See, e.g., EDPS Opinion of 22 December 2005–European Central Bank Internal Administrative Inquiries, (2005-0290).

- Concerned Head of Sector,
- Head of the Human Resources Sector,
- Head of the ITFM Sector,
- ICT Security Officer,
- IT System Administrator,
- IT service providers.

The EDPS highlights that Article 7 of the Regulation foresees that personal data be transferred "*for the legitimate performance of tasks covered by the competence of the recipient"*. In order to comply with this provision, in sending personal data, ERA must ensure that *(i)* the recipient has the appropriate competences and *(ii)* the transfer is necessary. An assessment of necessity of the transfer (and of the data being transferred) has to be carried out by the controller on a case by case basis.

In the case in point, the Head of ITFM, the System Administrator and the ICT Security Officer appear to be the persons responsible for managing internally the monitoring of e-mail use. The Head of Administration is, on the other hand, the controller of the processing operations related to administrative inquiry and disciplinary measures. The EDPS recommends ERA to revise the list of the recipients in the light of the above and evaluate on a case by case basis whether transfers from the ICT Security Officer, the System Administrator or the Head of ITFM to such recipients comply with Article 7. Indeed, only the persons responsible for deciding whether an administrative inquiry must be launched and for managing the system seem to be competent in the light of Article 7.

Furthermore, in particular circumstances the data may be disclosed on a temporary basis to the following categories of recipients within the European Union institutions and bodies:

- OLAF and/or IDOC within the frame of their inquests,
- the Ombudsman, at his request,
- the European Data Protection Supervisor, at his request.
- the Judges of the European Court of Justice, upon request,

The EDPS considers that the transfers of information to OLAF, IDOC, the European Court of Justice, the Ombudsman and/or the EDPS for the purposes of the performance of their official tasks comply in principle with Article 7. The assessment of necessity must, however, be performed by ERA on a case by case basis.

The notifications also mention transfers of data to the Prosecutor's Office. Transfers of data to the Prosecutor's Office will be dealt with in the frame of the prior checking Opinion on administrative inquiry and disciplinary proceedings. Indeed, such transfer will only take place where the administrative inquiry leads to the conclusion that a staff member may have committed a criminal offence.

According to the notifications, no transfers to third countries or international organisations are foreseen.

3.7. Rights of access and rectification, blocking and erasure

According to Article 13 of the Regulation, the data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge, from the controller, communication in an intelligible form of the data undergoing processing and any available information as to their source.

The EDPS recalls that the right of access is of a mandatory nature, unless an exception applies, and ERA has to put in place the procedures allowing its exercise. The right of access comprises, among others, the right to be informed and obtain a copy of the data that is being processed about an individual in an intelligible form. ERA must implement the appropriate procedures to ensure the possibility for users to exercise their right of access. The EDPS takes good note of the fact that data subjects can exercise their rights by sending an e-mail to a functional mailbox and that ERA undertakes to answer the request within one month.

In some instances the data controller may be able to rely on some of the exceptions contained in Article 20.1 of the Regulation to defer the provision of the rights of access or rectification. Notably, in this case, this may be lawful where such a restriction constitutes a necessary measure to safeguard *"(a) the prevention, investigation, detection and prosecution of criminal offences"*. In deciding whether to rely on an exception, ERA must engage in a case-by-case assessment of the circumstances of the particular data processing at stake.

If ERA uses an exception to defer the provision of access, it should take into account that the restrictions to a fundamental right cannot be applied systematically. ERA must assess in each case whether the conditions for the application of one of the exceptions. In addition, as foreseen in Article 20 of the Regulation, the measure has to be "necessary". This requires that the "necessity test" has to be conducted on a case-by-case basis. If ERA uses an exception, it must comply with Article 20.3 according to which *"the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor*". However, ERA may avail itself of Article 20.5 to defer the provision of this information as set forth in this Article: *"Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect."*.

According to Article 14 of the Regulation individuals have the right to rectify inaccurate or incomplete data. Due to the nature of the data (log files linked to users ID and IP addresses) and the way in which they are collected (logged automatically), the possibility of rectification of the data would appear unlikely. However, as a matter of principle, ERA must recognise the existence of such right which, in some limited cases may apply, for example, if someone makes use of someone else's user ID. The functional box can also be used for the purpose of deletion and rectification requests and an answer has to be provided, according to the notifications, within 3 calendar months.

The EDPS draws the attention of ERA on the rights to erasure and blocking pursuant ot Articles 16 and 15 of the Regulation. The data subject shall have the right to obtain the erasure of the data if their processing is unlawful. Pursuant to Article 15, the data subject shall have the right to obtain from the controller the blocking of data when their accuracy is contested for the period enabling the controller to verify the accuracy, the controller no longer needs them but have to be maintained for the purpose of proof, the processing is unlawful and the data subject opposes their erasure and demands the blocking.

3.8. Information to the data subject

Pursuant to Articles 11 and 12 of the Regulation, those who collect personal data are required to inform individuals that their data are being collected and processed. Individuals are further entitled to be informed of, *inter alia,* the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to.

In order to ensure compliance with Articles 11 and 12, ERA has taken (or will take) the following steps:

- ICT users will be officially informed of the monitoring procedure with a Note to the Staff on the "Use of ERA's ICT owned resourced".
- Furthermore, within a deadline of 30 days after the entry into force of the ICT, any existing user must sign the "ERA User acknowledgement Form" (the "Form"). New users must sign the same Form before access is given to ERA ICT resources. The form contains a confirmation that the user has read, understood and agreed to the ICT.
- All the set of policy documents is available at the intranet site of ITFM in the section DRAFT Policies – ERA Consultation.
- A specific awareness program that is part of the Electronic Information Security Program will be organised by the IT Security Officer in the coming months.

3.8.1. The information channels

The EDPS highlights the need for ERA to ensure that the channel selected to communicate the monitoring enables individuals to take cognisance of its content in an effective way. In the EDPS view, the following two aspects need to be taken into account.

First, in order to be effectively informed, users must receive direct notice of the processing which is taking place concerning their personal data. As most of the information is included in the policy documents, their publication on the Intranet does not seem sufficient, as not every user would spontaneously check it. As long as this has not been done, the EDPS therefore urges ERA to send an individualised notice to all staff, e.g. an e-mail message, displaying a link to the relevant Privacy Statement and the relevant policy document.

Second, the relevant documents provide the relevant information in a very disperse manner; indeed, to have access to the legally mandatory information, the user has to read at least six separate documents: the Note to the Staff, the Privacy Statement, the Internet Policy, the IAM policy, the ICT policy, the E-mail policy and the ECP. In some cases, the relationship between the various documents may not be self-evident.

In the EDPS view, it would have been preferable to provide the relevant information, including the content of Articles 11 and 12 of Regulation (EC) No 45/2001, in a unified way (rather than in different documents). This may have an impact from the point of view of fairness and transparency principles. In order to avoid confusion and enhance the intelligibility of the policies, the EDPS would suggest unifying all the information concerning the monitoring of e-mail in a single document containing all the necessary information (see further 3.8.2.). This document may be combined with a Privacy Statement.

3.8.2. The content of the policy

The main goal of ICT policies is to inform users of the authorised and prohibited use of the ICT, illustrate the type of monitoring which is carried out on the use, and highlight the consequences of a misuse or abuse. Having regard to ERA's Internet Policy, the EDPS has the following main remarks:

- Both the ICT and the E-mail Policy set out that ERA's ICT should be used for official business purposes and that only limited personal use is allowed, insofar as this does not

encroach upon ERA's interests. The concept of "limited personal use" is not further specified.

- The purposes for engaging in e-mail monitoring do not seem always clearly spelled out. In particular, the Policy states clearly that the monitoring of the log records may be performed with a view to ensuring the functionality and security of the systems but does not seem to be clear on the verification of authorised use/investigating purposes. Insofar as monitoring is aimed also at verifying authorised use, this has to be mentioned in an explicit manner.

Having regard to the Privacy Statement, the EDPS notes that it does not contain all the information requested for the purposes of Articles 11 and 12. In particular, there is not sufficient information on the (i) purpose of the processing, (ii) recipients (iii) categories of data, (iv) existence of the right of access. The additional information which may be considered necessary having regard to the specific circumstances to guarantee fair processing (such as legal basis, retention period, right to have recourse to the EDPS, etc.) is also missing.

The EDPS therefore invites ERA to remedy these shortcomings in order to align the Privacy Statement to the requirements of Article 12 of the Regulation.

3.9. Security measures

According to Articles 22 and 23 of the Regulation, the controller and the processor must 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 must 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.

ERA confirmed that it adopted the security measures required under Article 22 of the Regulation and these are detailed in the EISP document. The EDPS has no reason to believe that these technical and organisational measures are not appropriate to ensure a level of security in line with the risks represented by the processing and the nature of the personal data to be protected.

However, the EDPS considers that, because the e-mail logs are used not only for pure security purposes but also for evaluation of behaviour, the security measures might need to be reinforced. In particular, the EDPS recommends the following measures:

1. regularly review the risk assessments that are described in the EISP (this could be done as a part of the information security plan described in that same policy);
2. ensure that e-mail logs are protected from unauthorised access, modification or deletion, even from the ICT Security Officer and the IT system administrators;
3. ensure that each access to the e-mail log files can be traced back to a specific individual
4. ensure that all accesses to the e-mail logs files are justified and follow a proper documented procedure;
5. that responsibilities with regards to security incident management, internal inquiries and investigations are clearly assigned to specific functions and follow proper documented procedures.

3. CONCLUSIONS

The notified processing operation can only be implemented if the recommendations contained in this Opinion are fully taken into account. To ensure compliance with the Regulation the

EDPS recommends ERA to:

- limit the use of consent to access to users' e-mail for business continuity purposes on the basis of the modalities and conditions described in Section 3.2.2.1.;
- extend to access to files stored in individual computers the same rules foreseen for access to e-mail in the absence of a user, as outlined in Section 3.2.2.2.;
- reform the E-mail policy in the part where it provides for the applicability thereof to personal webmail accounts (Section 3.2.3.);
- reform the ECP provision stating that "*ERA post-holders are prohibited from seeking out, using, or disclosing personal information in electronic communications without authorisation*" (Section 3.2.3.);
- reconsider the definition of "Agency Electronic Communication Record" in a way consistent with the notion of public document covered by Regulation 1049/2001 on the public access to documents;
- remove or clarify the provision of the ECP stating that Agency Electronic Communication Records may include personal electronic communications (Section 3.2.4.);
- remove the provision of the ECP concerning interception of electronic communications;
- put in place technical and procedural safeguards to ensure that processing of special categories of data in the context of e-mail inspections or monitoring is kept to a minimum and occurs only where it is really unavoidable;
- perform individual examination of electronic communications data relating to e-mails, including content, only in presence of an adequate suspicion of wrongdoing which is corroborated by concrete initial evidence and in the framework of an administrative investigation. Such monitoring should be put in place only after available less intrusive means have been considered or tested. A clear procedure should be set up in this regard based on a gradual and proportionate approach;
- concerning access without consent, further specify and narrow down terms such as "compelling circumstances", "time dependent, critical operational circumstances" and "emergency circumstances;
- retain e-mail traffic data (including log files) no longer than six months after collection in compliance with Article 37(2) of the Regulation, unless they need to be kept for a longer period to establish, exercise or defend a right in a legal claim pending before the court;
- ensure that data transfers comply with Articles 7 and 8 of the Regulation, by means of a concrete assessment of their necessity;
- consider unifying all the information concerning the processing of data relating to e-mail use in a single document containing all the necessary information;
- integrate and/or clarify the E-mail Policy and the Privacy Statement in line with the recommendations made in Section 3.8.2.;
- regularly review the analysis performed to define to necessary controls that need to be implemented in order to reduce the risks to a level acceptable by management;
- reinforce security measures with regard to e-mail log files by ensuring the traceability of processing operations and access on a strictly need to know basis;
- clearly define all responsibilities that grant access to staff's personal data.

Done at Brussels, 6 December 2012.
(**signed**)
Giovanni BUTTARELLI
Assistant European Data Protection Supervisor