Opinion on the notification for prior checking from the Data Protection Officer of the European Railway Agency (ERA) regarding the use of ERA's Internet system.

Brussels, 6 December 2012 (case 2012-0135)

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**") a notification for prior checking relating to ERA's Internet system. Before filing the notification, ERA consulted the EDPS on the need for prior checking pursuant to Article 27(3) of Regulation EC 45/2001 (hereinafter the "**Regulation**"). The notification was 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 EDPS requested ERA to provide some complementary information on 2 April, 2 July, 7 and 28 September, 17, 23 and 26 October 2012. The answers were received on 4 May, 5 and 25 September, 15, 17, 18 and 24 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 further clarify some pending questions. The draft Opinion was sent to the DPO for comments on 15 November 2012. The EDPS received a reply on 4 December 2012.

2. FACTS

The present prior-check Opinion concerns ERA's Internet policy, as described in the Internet Policy and the ECP. According to ERA, the organisational part of the institution or body entrusted with the processing is the Administration Unit.

In addition to this specific notification, ERA transmitted as background documents to the EDPS its written policies concerning ICT, IAM and EISP. While these documents do not

[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.

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 Internet policy declared by ERA are the following:

- outline appropriate and inappropriate use of the Agency's Internet services;
- ensure that Agency's systems and Internet services are used for purposes which are appropriate to the Agency's mission;
- inform the Agency's community about the applicability of rules and ERA's policies when accessing Internet systems and services;
- prevent disruptions and misuse of ERA's infrastructure.

Appropriate and inappropriate use of the Internet

Section IV of the Internet Policy ("Allowable Use") outlines what according to ERA has to be considered as appropriate and inappropriate use. According to the document, any improper use of the Internet jeopardises the Agency's legal standing and shall not be tolerated. The document further defines "inappropriate use" as including, but not limited to, the following:

a. the Internet may not be used for illegal or unlawful purposes when accessed through ERA's infrastructure.[3]
b. the Internet may not be used in a way that violates ERA's policies, rules or administrative orders or in a manner which is inconsistent with the mission of the Agency.
c. individuals should limit their personal use of ERA's infrastructure to access the Internet. ERA allows limited personal use for communication with family and friends, independent learning, and public service. ERA prohibits use of mass unsolicited mailings, access by non-employees to ERA resources and network facilities, competitive commercial activity, and the dissemination of chain letters.
d. individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to ERA or another member of staff without permission.
e. users should not send unreasonably large electronic mail attachments.

Section V of the Internet Policy outlines additional rules regarding Internet security. Among others, it provides that:

a. accounts or password information cannot be shared;
b. downloading of software is not allowed;
c. when a new program or update of existing software seems to be necessary, the matter should be referred to the ICT Service Desk.

Monitoring of use

The ICT indicates that the Agency shall routinely monitor usage patterns of the ICT resources in order to ensure the functionality of ERA's information and information systems and avoid security breaches. In any case, the content of communications will not be subject to any monitoring. Derogations from the rules must be justified by the needs of the service and explicitly authorised by the Head of ITFM[4] and/or the ICT Security Officer, after consulting the IT Governing Committee.

[3] Including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. by means of viruses).
[4] IT and Facility Management.

All incoming and outgoing Internet traffic is automatically processed by one or more security tools to detect viruses, malware or spyware. All incoming Internet traffic from outside the Agency will be automatically scanned by anti-virus software. When a problem is detected, automatic disinfecting will be carried out.[5]

The Agency will use software filters and other techniques to restrict access to inappropriate information. When access is denied, the user will receive a clear and personal message showing the reasons why the access was refused. The access attempts will be consequently logged for the aforementioned purposes. ERA declared that the logs are not used to monitor individual behaviour, except those cases stated in Article 20 of the Data Protection Regulation. ERA provided in the Annex to the policy a list of filtered categories.

According to the Internet Policy, ERA may monitor any Internet activity occurring on ERA's equipment or accounts. The Agency keeps the logs of Internet traffic in order to ensure the functionality of ERA's systems and avoiding security breaches. Log files include the following:

- URL Access Log: name of ERA server processing the request, Date and Time, Client IP, Server IP, Domain, Path, Category, Protocol, number of hits, MB received. The client IP is leased dynamically;
- URL Blocking Log: Date and Time, Category, Rule, Scan Type, IOOID, URL, Protocol;
- URL Filtering Log: Date and Time, Category, Rule, Scan Type, Filtering action, URL, Protocol.[6]

It should be noted that ERA does not keep the logs from the service allocating IP addresses (DHCP logs).

2.2. Categories of data subjects

The categories of data subjects involved are the following:

- ERA's staff,
- ERA's contractors,
- individuals engaged in a professional collaboration with ERA, and
- any individual accessing any Internet services through the infrastructure provided by the Agency.

2.3. Categories of personal data

According to the notification, the categories of data involved are the following (i.e. data fields registered by the system):

- name of the ERA server processing the request,
- IP Address,
- timestamp of the processing of the requests (reception, assignation, modification, resolution, etc…),
- information related to the requested/accessed service,
- any information that the data subject provides within the transaction.

[5] Internet Policy, p. 10-11.
[6] Ibid., p. 11.

2.4. Data transfers/recipients

The notification indicates that the recipients are the ICT Security Officer and the Head of ITFM.

In further exchanges with the EDPS, the controller added the following internal recipients:

- Executive Director,
- Data Protection Officer,
- Head of Administration Unit,
- Concerned Head Unit,
- Concerned Head of Sector,
- Head of the Human Resources Sector,
- IT System Administrator,
- IT service providers.

In particular circumstances, data may be disclosed on a temporary basis to:

- judges of the Civil Service Tribunal, upon request, or
- the Prosecutor's office upon request, or
- OLAF and/or the IDOC within the frame of their inquiries, or
- the Ombudsman, at his request,
- or the European Data Protection Supervisor, at his request.

The notification also mentions transfers of data to the Prosecutor's Office.

2.5. Conservation of data

Log files (and other data concerned) are processed and retained for a maximum of 90 days.

2.6. Rights of the data subjects

The notification states that data subjects have been informed by means of a Note to the Staff entitled “Use of ERA’s ICT owned resources”, the ICT and the Internet Policy.

The data subjects can exercise their rights of access and rectification by sending an email to a functional mailbox with the specification of the right they want to exercise. The request will be dealt with by the data controller within one month or three months, according to whether the request is about access or blocking/erasure.

2.7. Security measures

Several system specific security measures are implemented and described in the Internet 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, incoming traffic from outside ERA's network is automatically scanned for and cleaned of viruses, malware and spyware;
- ERA uses filtering software to restrict access to inappropriate information (e.g. material that is obscene, racist, promotes terrorism ...);
- access to log files is reserved to ERA'S ICT system administrators and the ERA IT Security Officer.

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 check Opinion relates to ERA's policies concerning Internet use within the Agency, 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

The Regulation 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 [EU] 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 [EU] 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 Internet entails the collection and further processing of *personal data* as defined under Article 2(a) of the Regulation. Indeed, as described in the notification, personal data of Internet users are collected and further processed. This includes IP addresses, URLs visited, date and time, Internet traffic data, etc. Even if the traffic and other data concerning the use of electronic communications are not directly linked to a specific user, anonymity can always be lifted if ERA decides to carry out an in depth inquiry by cross-referencing the Internet logs with logs from other ERA systems. Data subjects are therefore identifiable.

In further exchanges with the EDPS, ERA clarified that the monitoring of Internet logs is carried out by automated means and "*anonymously"* as ERA specified that IP addresses are leased dynamically to clients and that it does not keep records on IP address assignation and lease (DHCP logs). Therefore, according to ERA, there is no possibility to trace back each Internet monitoring record to an individual computer. However, it is the EDPS point of view that ERA could use other logs (for example, e-mail logs, IAM logs...) to correlate the information contained in the Internet logs so as to trace back the majority of individual accesses to the Internet. Not having the DHCP logs means that some of the Internet accesses might not be easily traceable but in practice, other ERA logs will provide sufficient information to determine which user had a specific IP address at a specific time.

Second, as described in the Internet Policy and other documents, the personal data collected undergo *"automatic processing"* operations, as defined under Article 2(b) of the Regulation. All the data is captured and analysed by automatic means. A specific subset of data may also be manually analysed by the system administrator where further analysis is necessary, for instance in cases of suspected dangerous content such as viruses and so on. Indeed, in these cases the personal information is first collected automatically directly from Internet users (automatic registering of log files) and is then analysed by the ICT System Administrator.

Finally, the processing is carried out by an EU institution/agency/body, in this case by the ERA, 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".* The processing of data in the context of communications networks has specific aspects as regards data protection, which led to a chapter being drafted specifically on those aspects (Chapter IV). In particular, Article 36 lays down the basic principle of confidentiality of communications and Article 37 lays down provisions on traffic data.

This special consideration of such data must be seen as constituting a specific risk within the meaning of Article 27(1).

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*".

The data subjects are not directly identified while general monitoring is performed, but - at a second stage - the individual monitoring (see gradual approach, point. 3.2.2.) of the use of the Internet as described in the Policy documents may lead to the evaluation of users' behaviour (to assess whether or not their use of the Internet is in line with the Internet Policy) and, 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. In principle, 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 deeply regrets in the present case that the notification was not submitted to him prior to the start of the processing operations.

3.1.3. Notification and due date for the EDPS Opinion

The notification was 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 180 days to obtain some complementary information.

Moreover, on 10 May 2012, in accordance with Article 27(4) 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 10 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. 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 public interest task 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*).

3.2.1. Legal basis

First, the EDPS notes that the Regulation contains in itself various provisions that are relevant for evaluating the lawfulness of the monitoring by ERA of Internet usage. 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 Internet is to prevent that these instruments are used in violation of law, ERA's policies or in a way that is otherwise not authorised.

In addition, Article 35 of the Regulation provides that "*[EU] institutions and bodies shall take appropriate technical and organisational measures to safeguard the secure use of the telecommunications networks and terminal equipment*". This justifies the processing of telecommunications data which is necessary to ensure the security of the telecommunications systems.

Moreover, Article 37(2) of the Regulation provides for an additional legal ground which authorises ERA to lawfully 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 Internet Policy.

Second, the EDPS notes 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 that could justify a proportionate processing. For example, ERA's duty to protect itself from liability deriving from workers' actions may also justify the processing. This may include the processing of sensitive data, in certain circumstances (see Section 3.3).

Finally, the EDPS notes that 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.

3.2.2. Necessity

As described above, one of the main purposes declared about this processing is to verify whether ERA users employ the ICT services in accordance with the permitted uses laid down in ERA's internal policy documents. The EDPS takes note that ERA considers as necessary to engage in some monitoring of the use of its ICT services including Internet systems, with a view to being able to prevent or detect violations of its policies or security breaches. Therefore, it appears that a selective and proportionate registration of log files and their analysis, at least to some extent, may be considered as necessary for the purpose of carrying out the task of ensuring a use in accordance with the Internet Policy and thus, for ensuring the overall security

of ERA's ICT resources.

Some monitoring is also considered as necessary for the purposes of enabling the employer, in this case ERA, where appropriate to exercise its duties 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, downloading pornography) it may not have the necessary evidence to open disciplinary proceedings.

In the light of the above, the EDPS takes note that the notified monitoring of the ICT use is considered as necessary for achieving the intended purposes of the policy. Thus, the EDPS considers that the requirements for compliance with Article 5(a) of the Regulation seem to be satisfied in principle.

However, it should be noted that monitoring across the board or very thorough monitoring of the use of the Internet by each individual is not justified. With regards to cases where the IT Security Officer has an adequate suspicion that an individual is engaged in misuse, the EDPS recommends implementing a policy consisting in *gradually* increasing the monitoring depending on the circumstances. This will ensure that the monitoring is not excessive since only those data would be processed which would be necessary for the intended purposes. If the Internet logs show a potential misuse of ERA Internet services, a first step could be to remind staff of the policies in place and the possibility of administrative action; if the Internet logs show a continued misuse of the same type, ERA may initiate an administrative inquiry and a selective monitoring following a proper documented methodology (see also chapter 3.4). Thus, individual monitoring of Internet use should only take place in the presence of a reasonable suspicion which is corroborated by initial evidence and in the framework of an administrative inquiry. The anonymity of the alleged suspect should not be lifted before the hierarchy has decided to open an administrative inquiry.

A clear procedure should be set up in this regard foreseeing this gradual approach. When a suspicion occurs, the IT manager may for example decide that the suspicion should be reported to the relevant hierarchy (e.g. the HR Director). The latter may then decide about further investigative steps, i.e decide whether to lift the anonymity or not in the context of an administrative inquiry.[7]

The EDPS reminds that the conduct of an administrative inquiry falls under the scope of a processing operation of general nature: administrative inquiries and disciplinary measures[8]. This processing operation should be prior checked separately by the EDPS as it is intended to evaluate data subject's conduct (Article 27(2)(b)) and implies the processing of data relating to suspected offences (Article 27(2)(a).

Therefore, in monitoring the use of Internet, ERA should always respect necessity and proportionality in line with the data quality principle.

3.2.3. Log files of failed web access attempts

The ERA Internet Policy provides that the log files of failed web access attempts "*will not be used to monitor individual behaviour, except those cases stated in Article 20 of the Data Protection Regulation*". Article 20 of the Regulation allows exemptions and restrictions to, among others, data quality principle (Article 4 of the Regulation), where such exemptions and restrictions constitute a necessary measure to safeguard, *inter alia*, criminal investigations or a

[7] See, e.g., EDPS Opinion of 10 November 2008–Internet monitoring by the Court of Auditors (C 2008-284), available on EDPS website.
[8] See EDPS Guidelines: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-04-23_Guidelines_inquiries_EN.pdf.

monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority.

As highlighted in a previous Opinion,[9] the EDPS considers that filtering technologies entail a preventive approach to the misuse of the Internet rather than a detective or repressive one. Whenever the access to a prohibited website is blocked, the EDPS takes the view that monitoring and punishing the mere attempt to access those websites would go beyond what is necessary for the intended purpose. If the individual user never succeeded in accessing or viewing the content of a given blocked website, there does not seem to be a legitimate need to process such a failed attempt.

In the course of the procedure, ERA declared that attempts to access blocked web sites are not logged for a punishing/monitoring purpose. Indeed, the only purposes are to evaluate the accuracy of the filters (i.e. if no logs of blocked accesses by category are kept it's not possible to know if the filter is working or not) and to allow access to mis-categorised sites that are blocked when they should not be blocked.

To the extent that these are the only purposes, the EDPS would recommend removing from the Internet Policy the exception regarding monitoring of failed attempts in cases stated in Article 20(1) of the Regulation.

3.3. Processing of special categories of data

The monitoring of the Internet use may reveal "sensitive" 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). For example, trade-union membership may be revealed in access logs which show that an official routinely accesses a particular trade-union website. The processing of sensitive data is in principle prohibited unless one of the exception 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 Internet use 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 includes compliance with the duties and obligations deriving from employment law, such as ERA's right to prevent the viewing of sexually offensive information in the workplace which would justify the processing of sensitive information, such as certain URLs visited, that may reveal that an employee is engaged in this type of activity. 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 procedures including the dismissal of employees who engage in unlawful activities.

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,

[9] cf Opinion 2008-284, p. 8-9.

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 the Internet monitoring is to ensure that Agency's Internet systems and services are used for purposes which are appropriate to the Agency's mission (verification of authorised use) and prevent disruptions and misuse of the Internet systems (security monitoring). As stated above, the EDPS is of the view that a certain monitoring of Internet use may be necessary for the achievement of these goals. However, the processing of personal data in this context must not be excessive. It must be appropriate and proportionate having regard to the aims pursued.

In assessing proportionality, account should be taken of the specific nature of the data being processed in the context of the Internet monitoring. Log files record in a very detailed manner the Internet activity of each user, including the websites visited, the number of hits, the connection times, the time spent on each particular website, etc. A particularly prudent approach is therefore required from an EU institution/agency/body both when designing its Internet policies and when applying them in practice.

In this regard, a clear procedure implementing the gradual approach explained in point 3.2.2 should be set up.

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"*. In this case, the data include essentially log files. 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 the data are collected and/or further processed.

According to the notification and the Internet Policy, log files are retained for 90 days after their collection. This timing is in line with Article 37 of the Regulation which provides for specific measures as concerns the conservation of traffic and billing data, and log files are included in such a definition. Article 37.2 of Regulation (EC) 45/2001 provides that traffic data may be processed for the purpose of budget and traffic management, including the verification of authorised use of the telecommunications systems. However they 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.

If monitoring of log files or traffic data leads ERA to suspect that an individual has infringed the Internet Policy, ERA will be allowed to keep the incriminating log files. In this context Article 20 of the Regulation is 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.[10]

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 ISP or the Staff Regulations and ERA has opened an administrative inquiry. At the end of the first six months, an assessment is required whether the data collected and verification carried out are such as to reasonably support the continuation of the investigation 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.

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/agencies/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).

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, the controller must ensure that *(i)* the recipient has the appropriate competences and *(ii)* the transfer is necessary.

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 Internet use. The head of administration is, on the other hand, the controller of the processing operations related to administrative inquiry and disciplinary measures. ERA must therefore analyse whether transfers from the ICT Security Officer, the System Administrator and the Head of ITFM to the list of recipients described in the facts comply with Article 7. The necessity of such transfers must be analysed in the light of the gradual approach explained above.

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 Article 7 conditions are fulfilled. In particular, only the persons responsible for deciding whether an administrative inquiry must be launched and for lifting the anonymity of the data seem to be competent in the light of Article 7.

At a further stage, in particular circumstances the data may be disclosed on a temporary basis to the following categories of recipients within the European Union institutions/agencies/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.

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

The EDPS considers that the transfers of information to OLAF and or IDOC, the European Court of Justice, the Ombudsman or the EDPS for the purposes of the performance of their official tasks comply with these requirements. The recipients have in principle the competence to perform the task assignment for which the data is transferred. The assessment of necessity must be performed by the controller on a case by case basis.

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 notification, no proposed transfers to third country or international organisations is foreseen.

3.7. Rights of access and rectification

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. In the case in point, anonymity of the data subject will only be lifted when ERA decides, on the basis of the data collected through the monitoring of internet use, to launch an administrative inquiry. Therefore, in practice, the rights of access and rectification cannot be exercised before launching an administrative inquiry.

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 the following steps:

- ICT users have been 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.
- finally, users trying to access a prohibited website are told that access has been refused and the reasons for refusal (the website belongs to a non-desired category with the name of the category). The message shows the reasons why the access was refused.

Once the gradual approach described in chapter 3.4 is implemented, and if the Internet logs show a potential misuse of ERA's Internet services, ERA will need to inform users of the rules

defined in the Internet policy and the possibility for the Agency to initiate an administrative inquiry.

3.8.1. The information channels

The EDPS highlights the need for ERA to ensure that the channel selected to communicate the monitoring must enable individuals to take notice 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 and to be fair to the data subjects, 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 yet, 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 four separate documents, the Note to the Staff, the Privacy Statement, the Internet Policy, the ICT, the ECP. In some cases, the relationship between the various documents may not be self-evident.

In the EDPS view, it is appropriate 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). In order to avoid confusion and enhance the intelligibility of the policy, the EDPS would suggest unifying all the information concerning the monitoring of Internet use in a single document containing all the necessary information (see further 3.8.2.). This document may be combined with a Privacy Statement making clear reference to it.

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, to 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 Internet 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 Internet 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. Should monitoring be aimed also at verifying authorised use, the EDPS recommends clarifying this in an explicit manner;
- the document does not lay down a clear methodology for Internet monitoring. This reflects the fact that such methodology has not been yet been put in place (see above Section 3.4.1.), essentially because Internet monitoring is essentially performed on an anonymous basis;

- the Internet policy clearly specifies the World Wide Web as in the scope of the policy but is does not specifically address other protocols (such as Instant Messaging, FTP...). The EDPS recommends clarifying the policy so as to include all Internet protocols.

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 these 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 Internet 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 Internet log files can be traced back to a specific individual;
4. ensure that all accesses to the Internet 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.

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 Regulation 45/2001 the EDPS recommends ERA to:

- remove from the Internet Policy the exception regarding monitoring of failed attempts in cases stated in Article 20(1) of the Regulation;
- implement a gradual approach for the monitoring of individual Internet use in line with Section 3.2.2 above. In particular, perform individual monitoring of Internet use only in

presence of a reasonable suspicion which is corroborated by initial evidence, in the framework of an administrative inquiry and where available less intrusive means have been deployed;

- ensure that data transfers comply with Article 7 of the Regulation, by means of a concrete assessment of their necessity;
- retain traffic data beyond six months, only insofar as they are necessary to safeguard "*the prevention, investigation, detection and prosecution of criminal offences"* (in line with Section 3.7.);
- revise the list of recipients in conformity with Section 3.6 above. In particular, only the persons responsible for deciding whether an administrative inquiry must be launched and for lifting the anonymity of the data seem to be competent in the light of Article 7;
- consider unifying all the information concerning the monitoring of Internet use in a single document containing all the necessary information;
- integrate and/or clarify the Internet Policy and the Privacy Statement in line with the recommendations made in Section 3.8.2.;
- reinforce security measures with regard to log files by ensuring the traceability of processing operations and access on a strictly need to know basis.

Done at Brussels, 6 December 2012

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor