EDPS Comments on the Commission policy on the internal use of email

1. Introduction

On 24 September 2009, the EDPS received a consultation under Article 28.1 of Regulation (EC) 45/2001 regarding the draft Communication from the President in agreement with Vice President S. Kallas relating to the Commission policy on the internal use of email (hereinafter "the policy"). The policy was adopted on 26 October 2009.

On the basis of the EDPS competence as established under Article 28.1 and Article 41.2 of Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter "the Regulation"), the EDPS will assess specific points of the policy in terms of personal data protection and privacy principles.

These points will have to be taken into account in the additional measures that will be undertaken to complement the policy framework and the effective implementation of the policy. This is without prejudice to the prior checking of the subsequent monitoring of emails pursuant to the application of the Commission policy (see below point 4 "Prior checking").

2. General overview of the policy

The Commission considers email to be a core communication service that is critical to the continuity of its operations and plays a key role in the conduct of its work. Like many other organisations, the Commission faces growing difficulties with email overload, the time spent managing mailboxes, the rising costs associated with transmitting documents via email and questions of legal liability relating to the transmission and retention of emails.

The purpose of the policy is to establish a reference framework which will be made operational through implementing measures to ensure a smooth transition from current operating practices to a more efficient electronic communications environment. The policy includes 2 annexes: "List of target operating parameters for future use of email" and "Email best practice guidelines".

3. Legal analysis

The EDPS welcomes the Commission's decision to put in place a policy on the internal use of email. Employees at the Commission and other users need to know not only what they are allowed to do when they use the email service provided by the

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

Commission, but also what is expected from them in terms of best practice. The EDPS attaches a great deal of importance to ensuring transparency.

To the extent that the internal use of email within the Commission and monitoring of the use of email in accordance with the policy set out, involve the processing of personal data by a European Union institution, Regulation (EC) 45/2001 will apply.

In what follows the EDPS will examine the application of the data protection principles as provided for in Regulation (EC) 45/2001 to the Commission policy.

3.1. Email privacy

The application of the data protection principles call for a balanced approach between the right for an institution to monitor the use of the email system and the right for the users to see their privacy respected. Monitoring of the use of the email system may only take place when it is absolutely necessary and for specified purposes.

The EDPS welcomes that the Commission policy guarantees the fundamental right to confidentiality and privacy in the use of the email system. The policy also provides that in exceptional cases, such rights may - in accordance with the applicable regulations - be limited, for example in cases of investigations concerning fraud and other illegal behaviour or in cases where there are grounds for suspecting abuse.

The policy provides that "*the Commission has the right to review any electronic files and messages in cases of suspected breaches of legal or security obligations and may check the contents of email messages under the conditions set out in the Commission investigation procedures. Subject to appropriate authorisation this may include access to email message content and attachments without prior notification*". Similarly, the Administrative notice foresees that *"In case of suspected abuse of ICT services, the Director-General concerned may submit a reasoned request to the Director-General of DG ADMIN to open an investigation into the use of ICT by a particular member of staff".*

However, neither the policy nor the Administrative notice contain criteria defining what is considered as "suspected abuse". For example, the draft policy provides that DG DIGIT will routinely monitor statistics of the global volume of email traffic in order to detect "*abnormal activity levels that could lead to delays or blockage of the email system, thereby affecting the continuity of the Commission's operations*". What is considered as "abnormal activity levels" is not defined. In this respect, the EDPS would welcome the establishment of threshold criteria which could trigger a possible investigation procedure. Such criteria should be notified to individuals.

The EDPS considers that the monitoring activities should respect the necessity and purpose limitation principles according to which monitoring can only take place when it is absolutely necessary and for specified purposes (see Article 4.1(b) of the Regulation: *"Personal data must be: (...) (b) collected for specified, explicit and legitimate purposes (...");* as well as Article 8.2 of the ECHR as interpreted by the European Court of Human Rights in cases such as the Copland v. UK case.

In line with the data protection principles, the EDPS would also recommend the practice of a preventive approach (such as blocking of abnormally heavy emails) rather than an investigative approach.

The EDPS considers that the implementation framework of the policy should also provide a more comprehensive specification as to the procedures put into place to detect misuse or abuse and notably (1) what are the Commission's investigation procedures referred to in section 9, and (2) the appropriate authorisation for access to email message content and attachments without prior notification (who issues the authorisation, what is the procedure, etc).

The policy reads as follows: *"[h]owever, all monitoring and investigation activities have to fully comply with data protection rules"*. This general statement should go along with a more accurate explanation of how data protection rules will be complied with.

3.2. Personal use

The EDPS welcomes that the policy considers as acceptable a limited, occasional, or incidental use of email for personal, non-professional purposes, as well as the fact that users may use their personal webmail services. In this last case, users are allowed such a use provided that they comply with the Commission's Administrative notice on acceptable use of the information and communication technology services[1]. In this regard, the Commission's Administrative notice provides that the *"Commission's ICT services may not be used for illegal or irregular purposes, in a way that might disrupt the functioning of the service itself or in any manner contrary to the interests of the Communities"*. Staff are reminded in particular of the obligations set out in the Staff Regulations of officials, specific rules laid down in Commission Decision 2001/844/EC on the creation, handling and distribution of classified information and the Optimal top guidelines for an effective email use at the Commission. The policy itself further defines practices contrary to the principles in the Staff Regulations or in other provisions applicable to officials and which are consequently prohibited (see section 6 "Legal Considerations").

The EDPS is therefore satisfied not only that a certain use of the Commission email system is tolerated for personal use, but also that irregular or unauthorised use is clearly defined both in the Administrative notice and in the policy. The EDPS would further advocate the use of enhanced notices reminding staff members of the use they can make of the email network and subsequent verification mechanisms put into place by the institution. Staff members should be updated on an ongoing basis about their rights and obligations.

As concerns the identification of personal emails, the draft policy stipulates that they *"should be clearly indicated as such either by using the message property settings or by use of a disclaimer or by an indication in the message header"*. The EDPS considers that the identification of personal emails has to be unified. In particular, the EDPS does not recommend the reliance on a disclaimer as the sole mean of identification, because this would involve opening the email. An indication in the message header should be favoured. The Commission could propose the use of a standard expression such as "private" or "private email".

[1] Administrative Notice No 45-2006/08.06.2006 “Acceptable Use of the Commission's ICT services (PC equipment, email and internet acess systems, telephone, fax and mobile phones)”.

3.3. Message storage

The policy defines rules as concerns message storage and archiving. Annex 1 further defines a mailbox automatic deletion time limit (Inbox - Read and Sent items) of 6 months on provisional basis, to be further defined after an operational impact analysis of the pilot project exercise. The EAS object lifetime limit as defined in the annex is 7 years.

The EDPS underlines that any automatic deletion of emails in the mailbox of the users should be accompanied by the deletion of any corresponding data in the servers of the Commission.

The EDPS notes that the policy does not refer to the time period during which traffic data will be kept in order, notably, to perform some sort of monitoring (see above). Hence, he calls upon the Commission to fix a deadline and to communicate this deadline to users.

In setting up a retention policy in line with Article 37.2 of Regulation (EC) 45/2001, the Commission must take the following into account:

First, as a general rule the Commission must set up a deadline during which it will keep traffic data. In doing so, the Commission may decide to keep the logs for a maximum period of 6 months. As a general rule, the data can not be kept for a longer period. To comply with this rule, it would be appropriate to delete the data periodically and automatically.

Second, if monitoring of traffic data leads the Commission to suspect that an individual has infringed the email policy or is engaged in other unlawful activity, the Commission will be allowed to keep the incriminating logs files in order to "*establish, exercise or defend a right in a legal claim pending before the court*". 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 email policy or is engaged in other unlawful activity and the Commission has opened an administrative inquiry. 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*". Thus where relevant, log files may be processed in the frame of an administrative inquiry, whether it be a criminal or disciplinary offence.

3.4. Encryption

The EDPS welcomes that the policy makes specific reference to encryption as a means to ensure the safe use of the tool. However, the EDPS would like to point out that more specification about the methodology and procedures used for encryption should be provided in the implementation framework.

Furthermore, the policy refers to the possibility for third parties to recover encrypted information when necessary. The EDPS questions this access by third parties and

invites the Commission to identify these third parties and determine under what conditions and according to which procedures they should be entitled to access encrypted data.

3.5. Other data protection aspects not addressed in the policy

The EDPS would like to recommend the Commission to include a specific reference, in the implementation framework, to certain data protection rights and obligations, as follows:
a) the obligation to provide a notice to the data subject containing certain information (Article 11 of the Regulation);
b) the mechanisms for the exercise of the data subject's rights (Article 13 to 18 of the Regulation).

The EDPS would also like to recommend to the Commission to envisage including a point on the procedure for the institution or for third parties to access email boxes of staff members in the event of death, prolonged absence or departure from the institution.

4. Prior checking

The EDPS has analysed the extent to which the policy may give rise to prior checking under Article 27 of Regulation (EC) 45/2001. Prior checking is designed to address situations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. Processing operations likely to present such risks are specified in Article 27.2 and notably cover a) "*processing of data relating 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 email to ensure compliance with the policy leads to the evaluation of users' conduct and, on the other hand, that such monitoring entails the collection of data related to suspected offences, in principle, such monitoring and related data processing operations are likely to be subject to prior checking ex Article 27.2 sub a) and b) of Regulation (EC) 45/2001. Therefore, the EDPS recommends that the Commission submits the prior check notification when it will have developed the implementation framework specifying all the details on how the monitoring operations and concomitant investigation procedures will take place.

Conclusions

The EDPS is of the view that the Commission should develop an implementation framework (e.g. Guidelines, Internal rules, etc.) to specify certain data protection aspects, in the light of Regulation (EC) 45/2001. In particular, this framework should:

- propose use of a standard expression such as "private" or "private email" for the identification of personal e-mails;
- fix a time period during which traffic data will be kept in order to perform monitoring;

- keep incriminating logs files only in order to "*establish, exercise or defend a right in a legal claim pending before the court"* or in the frame 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 email policy or is engaged in other unlawful activity and the Commission has opened an administrative inquiry;
- adopt criteria defining what is considered as a "suspected abuse", as well as "abnormal activity levels". In this respect, the EDPS would welcome the establishment of threshold criteria which could trigger a possible investigation procedure;
- respect the necessity and purpose limitation principles according to which monitoring can only take place when it is absolutely necessary and for specified purposes;
- follow the practice of a preventive approach (such as blocking of abnormally heavy emails) rather than a investigative approach;
- provide a more comprehensive specification as to the procedures put into place to detect misuse or abuse, and notably (1) what are the Commission's investigation procedures referred to in section 9, and (2) the appropriate authorisation for access to email message content and attachments without prior notification (who issues the authorisation, what is the procedure, etc);
- provide more specification about the methodology and procedures used for encryption;
- include a specific reference to certain data protection rights and obligations, in particular the obligation foreseen in Article 11, as well as the rights of the data subject, foreseen in Article 13 to 18 of the Regulation;

Finally, the monitoring and related processing activities, referred to in point 4, has to be submitted to prior check, in the light of Article 27 of the Regulation.

Brussels, 1 February 2010