



PETER HUSTINX
SUPERVISOR

Mr. Jonathan STEELE
Data Protection Officer
of the European Parliament
Plateau de Kirchberg
B.P. 1601
L-2929 Luxembourg

Brussels, 4 May 2004

Dear Mr. Steele,

You have made a notification for prior checking in the sense of Article 27 (3) of Regulation (EC) No. 45/2001, which was received on 15 March 2004.

Please find enclosed my opinion concerning the lawfulness of the processing operation which was the subject of your notification.

The opinion concludes that the proposed processing does not seem to involve a breach of any provision of Regulation (EC) No. 45/2001, provided that its considerations are fully taken into account.

Please let me know if this opinion gives rise to any questions, and keep me informed about any aspects of the proposed processing that you may want to bring to my attention.

Yours sincerely,

Peter HUSTINX



OPINION on a NOTIFICATION for PRIOR CHECKING
received from the Data Protection Officer of the European Parliament

Brussels, 4 May 2004 (Case 2004/13)

Proceedings

1. On 1 March 2004 a consultation in the sense of Article 27 (3) of Regulation (EC) No 45/2001 was received from Mr. Jonathan STEELE, Data Protection Officer of the European Parliament:
 - On 10 February 2004 the EP's Directorate for IT had asked the DPO for an opinion on the lawfulness of a proposed investigation intended to verify the truth or falsity of accusations made against a certain official by a third party outside the EP, about the abusive use of his/her Internet connection and email tool. The investigation would involve checking the Internet connections and traffic data about e-mails (presumably both sent and received) over a three-month period.
 - The DIT had informed the DPO that the EP's Secretary General had asked it to provide, with due respect for dispositions concerning personal data protection, statistics on Internet connections of the above mentioned official over a three-month period and a similar analysis of his/her email traffic, with a view to either exonerate the official or take the appropriate measures against the abusive use.
 - On 20 February 2004 Mr. STEELE had delivered his opinion to Mr. Pierre JEGU, Chief of Division of the EP's DG1/DIT/GITI. The DPO felt that the processing could only be lawful on the basis of Article 20 (1) of Regulation (EC) No. 45/2001 and that, as the investigation could potentially, depending on the facts brought to light, result in disciplinary proceedings against the official in question, the proposed operation would present "specific risks to the rights and freedoms of data subjects" in the sense of Article 27 of the Regulation, and should therefore be subject to prior checking by the EDPS.
 - At the same time, the DPO suggested the possibility of a preliminary indication of the EDPS concerning the interim retention of traffic data, to avoid its deletion before an opinion on the lawfulness of processing was delivered.
2. On 4 March 2004 a videoconference took place between Mr. JEGU (in Luxembourg) and Mr. HUSTINX, EDPS, Mr. BAYO DELGADO, Assistant EDPS, and Mr. STEELE (in Brussels) to clarify the issue. No further details were available on the case. After the videoconference, the EDPS expressed his opinion that, in view of the circumstances, a prior checking seemed appropriate, subject to a notification with all necessary details on the processing operation involved. Mr. JEGU was also to inform, as soon as possible, on the

present practice concerning the processing of traffic data and the period of their retention, in the absence of the list referred to in Article 37 (2) of the Regulation.

3. On 10 March 2004 Mr. STEELE informed the EDPS by e-mail that the information available at that point was that Ms. D - the official concerned - had asked the EP for support under Article 24 of the Staff Regulations. This provides for the Communities to assist a staff member if he/she suffers threats or insults "by reason of his position or duties". Ms. D. was, according to her statement, suffering a campaign of harassment from Mr. X, in the form of constant e-mails and his giving her EP e-mail address in Internet chat-rooms. The case had now been mentioned in the pages of the satirical publication called "The Sprout". It seemed that criminal proceedings were already, or were about to be, under way in Belgium, being Ms. D. the instigator. A copy of an email sent by Mr. Pierre LORA-TONET addressed to Mr. JEGU and others was attached.
4. On 12 March 2004 Mr. STEELE sent a PDF copy of the above-mentioned publication to the EDPS.
5. On 15 March 2004 a notification for prior checking in the sense of Article 27 (3) was received by the EDPS from the DPO of the European Parliament. Attached, besides other communications already mentioned, there were a copy of a note of Mr. Roger Vanhaeren, Director General of Finances, to the attention of Mr. Julian Priestly, EP's Secretary General, dated on 9 March 2004, and a copy of Ms. D's Article 24 request to EP's SG, of 8 March 2004, in which she expresses to be ready to give her consent "pour que la DIT fasse toutes le vérifications utiles sur mon ordinateur et vérifier mon trafil (sic) e-mail, si la demande devait m'en être faite".
6. On 16 March 2004 Mr. JEGU informed the EDPS, via Mr. STEELE, that the traffic data retained are:
 - Email: sender's address, receiver's address, date and hour of transmission, message size; retention period: 3 months.
 - Internet connections: address IP of post, visited site address (URL), date and hour of hit, size of exchanged packages; retention period: 6 months.
7. On 24 March 2004 the EDPS gave a favourable indication as to the retention of the above-mentioned data, at least until a final opinion had been given on the lawfulness of the proposed processing.

Facts

8. As far as known until now, the facts are as follows. Ms. D. has asked the European Parliament for support under Article 24 of the Staff Regulations, as, according to her statement, she is suffering since the beginning of January 2004 a campaign of harassment from Mr. X. This harassment is claimed to take the form of constant e-mails and his giving her EP e-mail address in Internet chat-rooms. E-mails have been sent to EP members and staff accusing her of misuse of her Internet connection and email tool. She is ready, if asked for, to give her consent for the DIT to make any necessary checks in her PC and e-mail traffic. It seems that judicial criminal proceedings against Mr. X are already, or are about to

be, under way in Belgium, being Ms. D. the instigator. The present practice of traffic data retention in the EP is 3 months for e-mail (sender's address, receiver's address, date and hour of transmission, message size) and 6 months for Internet connections (address IP of post, visited site address (URL), date and hour of hit, size of exchanged packages).

Legal aspects

a) Prior checking

9. Article 27 (1) of Regulation (EC) 45/2001 subjects to prior checking by the EDPS all "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. In the English version and a number of other versions of the Regulation, this list appears not to be a *numerus clausus*. The French version is not so clear in that respect. Systematic interpretation however leads to the conclusion that there may well be other cases in which specific risks are likely to be present which justify prior checking. Although this case was not within the cases listed in Article 27 (2), the consultation on the need for prior checking was therefore appropriate.
10. The processing of traffic data presents specific problems, which are so important that they deserve a separate provision and special safeguards in the Regulation, such as the list provided for in Article 37 (2), which has not yet been established. Furthermore, the proposed processing may have significant and serious consequences for each of the data subjects involved, the EP official and her suspected harasser, namely disciplinary measures and criminal or civil liability, even apart from the breach of the confidentiality of their communications also in other respects. According to Article 27 (1) of the Regulation the prior checking was therefore necessary.
11. The notification of the DPO was received on 15 March 2004. According to Article 27 (4) the present opinion has to be delivered within a period of two months, that is before 15 May 2004.

b) Data retention

12. This opinion does not intend to analyse the processing of traffic data as such and the conditions in which the retention of these data is lawful in general terms. This opinion is limited to the processing operation, which was the subject of the notification for prior checking.
13. In the absence of a list of data agreed by the EDPS to be processed for the purpose of telecommunications budget and traffic management, including the verification of authorised use of the telecommunications systems, the erasure of traffic data as prescribed by Article 37 (1) can be postponed under Article 20 (1)(a) and (c), where this is necessary for the purposes indicated, as Article 37 (1) is mentioned among the possible restrictions.
14. The data kept by the European Parliament's DIT in the present case seem reasonable and appropriate. The data retained are not excessive for the verification of abusive use of the Internet and e-mail tools. For this specific purpose, the exclusion of some of the data, such

as the email receiver's address or the visited Internet site addresses, would mean crucial impossibility of obtaining conclusions on the authorised use of the telecommunication system. As to the period of retention, it is within the six months after collection allowed by Article 37 (2) of the Regulation. This means that the processing of the retained data by the DIT must in principle take place within such period. Only in the case that there is formal notice of judicial proceedings on the issue, those data should, where necessary, be kept as long as needed for the conclusion of such proceedings.

c) Lawfulness of processing

15. The analysis of traffic data is clearly an operation that comes under the definition of "processing" of Article 2 (b) of the Regulation. Furthermore, sender's and receiver's addresses and address IP of post are personal data. As far as the other data are linked to those, all of them come under the definition of "personal data" of Article 2 (a). The same applies to statistics on the Internet connections or email traffic of identifiable individuals.
16. Traffic data as such are not included in any special category of data, as defined in Article 10. Consequently, no prohibition or limitation as provided for in Article 10 is applicable.
17. As to the lawfulness of processing such data, it is covered by the legitimate exercise of the official authority vested in the European Parliament, as a Community institution, to guarantee the proper use of the tools at the disposal of its civil servants and other personnel, on the basis of Article 5 (a). In fact, Article 37 (2) implies the lawfulness of such processing in principle, including the receiver's address of outgoing traffic as a substantial element to judge on the proper use of the e-mail system.
18. In this case, lawfulness also results from the performance of a task carried out in the public interest on the basis of Article 24 of the Staff Regulations, as the European Parliament has the legal obligation to "assist any official, in particular in proceedings against any person perpetrating threats, insulting or defamatory acts or utterances, or any attack to person or property to which he or a member of his family is subjected by reason of his position or duties" (Article 24 of the Staff Regulations).
19. The processing operation, presently under consideration, seems reasonably necessary for the proper execution of the task of the European Parliament in both perspectives. The emphasis on "statistics on Internet connections and email traffic" suggests that data will not be investigated or presented in unnecessary detail. In any case, where possible, investigation and reporting should respect the principles of proportionality and relevance.
20. It should be noted that Article 37 (3) provides for special safeguards with respect to the persons accessing and further processing traffic data. Other persons should not handle these data.

d) Compatible use

21. Traffic data relating to users are, according to Article 37 (1), in principle only processed to establish calls and other connections over the telecommunications network. These data therefore benefit from all measures to secure the security and confidentiality of communications as referred to in Articles 35 and 36. However, subject to certain conditions and safeguards, those data may, if necessary, also be processed for the purpose of

telecommunications budget and traffic management, including the verification of authorised use of the telecommunications systems, on the basis of Article 37 (2).

22. In the absence of a clearly developed framework for such use, it is important to observe that the traffic data referred to before may be used to carry out the proposed investigation under Article 20 (1)(a) and (c) in relation to Article 4 (1)(b) of the Regulation, where this is necessary for the purposes mentioned in the former provisions.
23. Article 6 (1) is not applicable, as it refers to a general change of purpose in the processing of collected data. Article 6 (2) is not applicable either, as traffic data are not "collected exclusively for ensuring the security or the control of the processing systems or operations".

e) Consent of data subject

24. In view of this analysis, there is no need for the data subjects' consent with respect to the proposed processing, but this prior checking was necessary due to specific risks to the rights and freedoms of both data subjects.
25. Nevertheless, if the EP decides to ask for the consent of both or either one of the data subjects under Article 5 (d) - so far only Ms. D has been mentioned in this respect - it has to very strictly fulfil the requirements of Article 2 (h) - any consent needs to be free, specific and informed - as the investigation may lead to negative results for the data subjects. The consent should also include Internet traffic, not mentioned by Ms. D. in her letter.

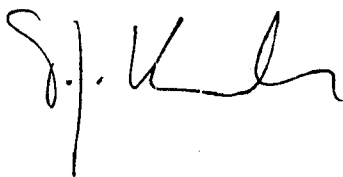
f) Information to data subjects

26. In the absence of consent, both data subjects have to be informed of the processing and the reasons thereof, according to Article 20 (3) of the Regulation, as well as of the existence of this prior checking, without prejudice to a possible recourse to the EDPS.

Conclusion

The proposed processing does not seem to involve a breach of any provision of Regulation (EC) No. 45/2001, provided that the aforementioned considerations are fully taken into account.

Done at Brussels, 4 May 2004



Peter HUSTINX