EUROPEAN DATA PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Ms Laraine LAUDATI
Data Protection Officer
European Commission
European Anti-Fraud Office (OLAF)
1049 Brussels
BELGIUM

[DPO of a European institution]

Brussels, 19 December 2013
GB/DG/sn/D(2013)0669 **C 2013-1320**
Please use edps@edps.europa.eu for all correspondence

Subject: **Consultation under Article 46(d) on access to traffic data in the context of an OLAF internal investigation**

Dear Ms Laudati and [DPO],

Thank you for your joint consultation on a matter concerning telephone traffic data which has arisen in the context of a European Anti-Fraud Office (OLAF) internal investigation into a former official of [a European institution].

Your consultation covered five separate points, which will be addressed in the "legal analysis" section of this letter.

Facts

In the context of an internal investigation into a former [institution] employee, OLAF performed an inspection of [institution] premises on [date]. On [date], OLAF investigators asked the [institution] to provide a complete copy of paper records, stored in accounting files, of professional telephone calls made by the person concerned during the period 2008-2011 on a mobile phone held by the [institution] and made available for use to that person. Officials of the [institution] confirmed the existence of such records.

The following day, the [institution] presented records to OLAF for the periods in question. These records contain the name, signature and phone number of the person concerned; date, time and duration of the calls; dialled numbers; type of calls (roaming, national, international, SMS); network used and cost of the calls. The records for 2008 may also include details about calls that the person concerned had designated as private. Following OLAF's request, the

records were initialled by the [institution]'s DPO and Head of IT infrastructure unit, as well as by OLAF investigators, with the understanding that they would be secured at the [institution] for possible future transmission to OLAF but subject to consultation of the EDPS. The EDPS understands, in consequence, that OLAF has not yet accessed any of this data, but has merely been made aware of its existence by the [institution].

In [year] the [institution] transmitted its notification concerning [the private use of professional mobile phones] to the EDPS, and the EDPS decided this processing operation was not subject to prior checking.[1] The notification specified that invoicing data would be retained for five years from the date of discharge by the European Parliament for the budgetary year to which the documents relate, while the traffic and location data would be erased or made anonymous as soon as possible, and no later than six months after their collection. The EDPS remarked in his letter that he considered the retention policy to be adequate and in accordance with the provisions of Regulation (EC) 45/2001 (the Regulation).

In fact, the traffic data requested by OLAF in July 2013 were retained by the [institution] together with the invoicing data for a period long exceeding the six month limit prescribed by Article 37(2) of the Regulation, despite the fact that they did not "need to be kept for a longer period to establish, exercise or defend a right in a legal claim pending before a court", as required by that provision.

Legal analysis

Article 4(1)(a) of the Regulation requires that personal data must be processed fairly and lawfully. Article 5 of the Regulation goes on to stipulate a number of conditions under which the processing of personal data can be considered lawful. Furthermore, Article 7 provides certain requirements for the transfer of personal data between Community institutions and bodies.

Given that the traffic data has been retained by the [institution] for a period beyond the six months prescribed in Article 37(2) of the Regulation, the EDPS is of the strict view that this data cannot be provided to OLAF in the context of its internal investigation. In this case, the transfer of the data would not be lawful under Article 5 of the Regulation as there is no legitimate legal ground for its transmission. This is because the prior retention of the data is in breach of Article 37(2), and as such, is neither lawful nor fair. In other words, the mere fact that the data has been retained breaches the data quality principle under Article 4, so that any further transfer of this data would consequently be prohibited.

OLAF and the [institution] also asked whether the exception under Article 20(1)[2] of the Regulation to the requirement of Article 37(1)[3] could now be invoked because retention of the data is "a necessary measure to safeguard (a) the prevention, investigation, detection and prosecution of criminal offences", despite:

- the fact that Article 20(1) does not contain any reference to Article 37(2) and;
- the fact that the [institution], before the expiration of the six month period, has neither adopted general rules concerning the application of a limitation under

[1] [...].
[2] Article 20(1)(a) allows restriction on the application of Article 37(1) among others, where this is necessary for the prevention, investigation, detection and prosecution of criminal offences.
[3] Article 37(1) provides that traffic data shall be erased or made anonymous upon termination of the call or other connection.

Article 20(1) and allowing the conservation of traffic data beyond the six month period, nor a specific decision pursuant to that provision allowing the conservation of traffic data of the person concerned.

Without prejudice to the validity of any exception the [institution] might have initially cited in order to exceed the six month retention period for the traffic data in question, the fact is that such an exception was never proposed or specified at that time, and therefore, is not relevant now. Any such exception should be proposed in advance, and not after the event. Data that *potentially* may or may not later be required for criminal purposes cannot be retained on a "just in case" basis, as this would contravene the data quality principle of the Regulation in terms of fairness and lawfulness. Moreover, it has already been confirmed by both OLAF and the [institution] that the traffic data in question was not originally retained because of any relation to criminal offences.[4]

This advice, and the conclusions and recommendations below, are without prejudice to any internal rules that may be adopted by the [institution] or OLAF in the future.

Another query raised by OLAF and the [institution] related to the potential application of Article 49, first subparagraph, point d), of Regulation (EC, Euratom) 2342/2002, notwithstanding the provision of the third subparagraph of that Article (see now Article 48, first subparagraph, point d), and third subparagraph, of Delegated Regulation (EU) 1268/2012). The EDPS does not consider that traffic data can be lawfully retained beyond the six month period, along with accounting data, for the purposes of this Article (which relates to the keeping of supporting documents by authorising officers). As explained in Regulation 1268/2012, personal data contained in supporting documents should be deleted when those data are not necessary for budgetary discharge, control and audit purposes. It also confirms that Article 37(2) of the Regulation shall apply to the conservation of traffic data. In this case, the telephone traffic data did not need to be retained for billing purposes under Regulation 1268/2012, and as such, there was no valid reason for keeping them.

With regard to the treatment of private versus professional calls, along with the matter of further retention periods imposed by OLAF on any data obtained from the [institution], neither of these issues are in fact relevant in this case, as it has already been established that none of the data in question can be legally processed.

Conclusions and recommendations

1. OLAF should not access the data currently being securely stored by the [institution], for the reasons outlined in this letter.
2. In future investigations, OLAF should not access any personal data retained beyond the periods as specified in the Regulation.
3. The [institution] should securely delete the traffic data in question, along with all other traffic data that has been stored for longer than the six month maximum retention period as stipulated in the Regulation (unless a court case is pending).
4. The [institution] should implement a formal system to ensure that the relevant retention periods for traffic data are respected from now on.

[4] See, by analogy, Judgment of the Court (Third Chamber) of 7 November 2013 in Case C-473/12, *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others.* The judgment concludes that Member States have the option, but not the obligation, to transpose into their national law one or more of the exceptions listed in Article 13 of Directive 95/46/EC. This highlights the need for an internal rule on the general application of exceptions.

We would be grateful if you would bring these recommendations to the attention of the controllers concerned. The EDPS should be informed of the implementation of these recommendations (with documentary evidence where available) as soon as possible, and no later than three months following receipt of this letter.

We hope that this answers your consultation, and we remain available for any additional queries or clarification. Thank you in advance for your cooperation.

Yours sincerely,

[signed]

Giovanni BUTTARELLI