Prior Checking Opinion

‘Management of incident reports– Court of Justice’
Case 2013-0786

***

The Court of Justice has entrusted a security firm with the task of drawing up reports in the event of incidents regarding any anomaly, malfunction, aid given to persons, or issue relating to the security or safety of persons, assets and buildings occurring within the Court. Those reports may contain personal data, for example regarding persons who are the victim of an accident or a fire or who are taken ill, or even persons who are disturbed whilst committing a theft at the premises of the Court.

***

Brussels, 12 September 2016

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
Email: edps@edps.europa.eu - Website: http://www.edps.europa.eu
Tel: 32-2-283 19 00 - Fax: 32-2-283 19 50

1. Procedure

On 27 June 2013, the European Data Protection Supervisor (**EDPS**) received from the Court of Justice of the European Union (**the Court**) a notification for prior checking under Article 27(2)(a) of Regulation No 45/2001 (**the Regulation**) concerning the management of incident reports.

The notification was accompanied by the following annexes:

- a description of security measures;
- the information note concerning the processing of personal data;
- the Regulation of the Grand Duchy of Luxembourg of 16 October 1997 on the protection of workers - Standard safety requirements (ITM-ET 32.10) (**Regulation ITM-ET**);
- an extract from security contract CJ 03/2010.[1]

Various exchanges of correspondence have taken place between the Court and the EDPS. Additional documents[2] and an amended notification were sent to the EDPS on 16 March 2016.

As this is an ex post prior checking, the two-month period within which the EDPS must, in principle, deliver its opinion does not apply.[3]

2. Relevant facts

In 2010, the Court entered into a contract with a security firm to provide general security and fire safety services. In that connection, the officers employed by that firm are required to draw up **incident reports** regarding any anomaly, malfunctioning, aid given to persons, or issue relating to the security or safety of persons, assets and buildings occurring within the Court. Those reports are sent by email to the Security and Safety Section (attached to the Court's Buildings Directorate) within 24 hours. Every morning on working days, a summary of the reports from the previous 24 hours is drawn up and sent by email to the Security and Safety Section. Approximately 1 500 to 2 000 incident reports are drafted each year.

2.1. Legal basis and lawfulness of the processing

According to the Court, the **legal bases** of the processing are:

- Article 26 of Regulation ITM-ET (Inspection du Travail et des Mines [Labour and Mines Inspectorate], Luxembourg); this provision concerns safety installations (fire safety, air monitoring and gas detection systems, etc.) and the requirement to keep records of checks carried out on those installations;

[1] The Court has subsequently submitted a copy of all of the relevant security contracts: contract CJ 03/2010, applicable from 16 December 2010 to 15 July 2015, and contract CJ 12/2014, applicable from 16 July 2015 to 15 July 2020.

[2] Incident report template; summary report template; extract from the call for tenders regarding the services provided by the security firm.

[3] The EDPS put a number of questions to the DPO on 18 December 2013, in addition to a reminder and a draft statement of facts on 16 October 2015. The DPO replied on 16 November 2015. The draft opinion was sent to the Court DPO on 16 June 2016. The Court submitted its comments on 5 August 2016.

- Article 4.2 of the tender specifications regarding the services provided by the security firm G4S Security Services; that provision requires the security firm to (i) put in place a computerised management system for incident reports and their follow-up; (ii) provide the Court with all of the activity reports it requires.

The initial notification also made reference to the '*Blueprint for the overall safety of the buildings complex of the Court of Justice of the European Union*'. The updated notification no longer refers to that document.[4]

The **lawfulness** of the processing is based on Articles 5(a) and 10(2)(b) of the Regulation.

2.2. Data subjects

The data subjects are persons involved in an incident in Court buildings or their immediate vicinity, regardless of whether or not they are Court staff.

2.3. Categories of data

The **incident reports** may contain the following personal data:

- contact details of persons involved in the incident (first names and surname, telephone and fax numbers, email address);
- information contained in the identity documents belonging to those persons (passport, driving licence, etc.);
- nature of the facts (accident, theft, aid given to a person, the victim's state of health, suspected offence, etc.);
- vehicle registration numbers;
- place, date, time and cause of the incident;
- damage observed and interim action.

In addition to the incident reports, every morning on working days the security firm prepares a **summary** of the reports drawn up in the previous 24 hours by regrouping them into five categories:
- technical incidents;
- incidents regarding fire safety;
- incidents regarding safety;
- aid given to persons;
- miscellaneous.

That summary consists of a table reproducing the number of incidents per category, the subject matter of each report, its number and observations.

2.4. Recipients of the data

The incident reports and summaries of the reports are transmitted in electronic form (email) in pdf format.

[4] See email from the DPO to the Court of Justice dated 16 March 2016.

The **recipients** of that data are:
- officials and agents of the Security and Safety Section of the Court;[5]
- the Director of Buildings;
- the security firm staff who perform the security roles;
- the administrative and prosecuting authorities in Luxembourg for the purpose of exercising their powers in the field of the prosecution of offences (recipients under the national legislation adopted in accordance with Directive 95/46/EC). Depending on the scope of the incident, the Security and Safety Section may transmit the report to those authorities.

Other recipients may receive the data in specific cases.[6]

2.5. Information provided to data subjects.

Court staff: an information note[7] and the notification of the processing operation are available on the Court's intranet.

Other persons: the information note is not available on the Court's website.[8] The security officers assigned to the public reception area have a paper copy of the note which is available to the public.

2.6. Storage, security measures and retention period for the data

[...]

The **retention period** for the reports is ten years and one day. According to the controller, that period, which does not follow from a legal requirement, is based on general use in the Grand Duchy of Luxembourg regarding the management of safety registers.[9]

No provision is made for a paper archive.

---

[5] The Court's Buildings and Security Unit, mentioned in the initial notification, has since been disbanded. The Security and Safety Section is now attached directly to the Buildings Directorate.

[6] - the President and Registrar of the Court and the officials who assist them in the context of the responsibilities devolved to them by Article 20(4) of the Rules of Procedure of the Court of Justice;
- the Court of Justice, the General Court and/or the Civil Service Tribunal, or a national court, in addition to lawyers and agents in the event of a dispute;
- the formation of the Court, General Court or Civil Service Tribunal responsible for examining claims, the President and Registrar of the court concerned and the legal advisor for administrative matters, in the event of a claim brought under Article 90(2) of the Staff Regulations of Officials;
- OLAF in the event of an inquiry under Regulation No 883/2013 and the Decision of the Court of Justice of 12 July 2011 concerning the terms and conditions for internal investigations in relation to the prevention of fraud, corruption and any other illegal activity detrimental to the interests of the European Union;
- the internal auditor in the context of the responsibilities devolved to him by Articles 98 and 99 of Regulation No 966/2012 on the financial rules;
- the EDPS in accordance with Article 47(2) of the Regulation;
- the Court DPO in accordance with point 4 of the Annex to the Regulation;
- the European Ombudsman in the context of Article 228 TFEU.

[7] Annexed to the notification.

[8] Information communicated by the DPO by email of 5 August 2016.

[9] Article 26 of Regulation ITM-ET provides that registers must be available to supervisory bodies, that is to say the Inspection du Travail et des Mines [Labour and Mines Inspectorate]. However, no retention period is stipulated.

3. Legal analysis

3.1. Prior checking

The processing of personal data is carried out by a European Union institution and performed in part by automatic means. Regulation (EC) No 45/2001 is therefore applicable. This processing activity is subject to prior checking by the EDPS since it presents specific risks related to the processing of data relating to health and to suspected offences (Article 27(2)(a) of the Regulation.[10]

3.2. Legal basis and lawfulness

Incident reports may be drawn up in very different circumstances and for very different purposes:
- technical safety of installations (including fires) and subsequently, indirectly, of persons;
- security of persons (whether employed by the Court or not) with no link to the installations (theft, etc.);
- health of persons (whether employed by the Court or not) with no link to the installations (illness, accident).

a. Legal basis

The Court mentions two legal bases in support of the processing:
- Article 26 of Regulation ITM-ET;
- Article 4.2 of the tender specifications regarding the services provided by the security firm 'G4S Security Services'.[11]

Having regard to its scope,[12] Regulation ITM-ET constitutes a legal basis for the processing only in respect of reports relating to the safety of installations. As for the tender specifications, these do not constitute a legal basis for the processing (reporting) in themselves, but solely the sub-contracting of that activity to the security firm.

Therefore, the Court must adopt an internal decision providing for reports to be drawn up for the various purposes described above.

b. Lawfulness

With regard to the **incident reports relating to the technical safety** of installations **and to fires**, the processing may be regarded as lawful under Article 5(a) (in the light of recital 27 of the Regulation).

[10] Pursuant to Article 27 of the Regulation, the EDPS shall carry out a prior check on any 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 lists the processing operations that are likely to present such risks and, in paragraph (a) in particular, the processing of data relating to suspected offences, offences, criminal convictions or security measures. However, processing operations that involve such data only exceptionally or on a one-off basis are not subject to prior checking. In the light of the information provided by the Court, this does not appear to be the case here and therefore the processing is subject to prior checking.

[11] See the summary of relevant facts, section 2.1.

[12] See Article 1 - Objective and scope.

The processing of data in **incident reports relating to health** (for example, an employee or outside person being taken ill), and in reports relating to **security with no link to the installations** (thefts and other offences in the buildings and the immediate vicinity) is lawful under the same provisions, subject to the adoption of an internal decision by the Court providing for such reporting (see point a. above).

The various types of report mentioned above may include data relating to health and suspected offences, including reports concerning the security of installations.[13] The processing of those categories of data is lawful under Article 10(2)(a) (in respect of persons outside the Court - if a valid consent has been given), (b) (in respect of Court staff) and Article 10(5). Therefore, in order to strengthen the lawfulness of the processing, in particular with regard to persons who are not Court staff, the aforementioned decision should expressly provide that the reports may contain that type of data.

The same rules apply to summaries of the reports in so far as they contain personal data.

Moreover, as stated in section 3.3 above, as far as possible, the **collection** of personal data, in particular those referred to in Article 10 of the Regulation, must be **limited**.

Recommendation

1. Adopt an internal decision providing for incident reports to be drawn up for the various categories of report set out above and authorising in that connection the processing of the special categories of data set out in Article 10 of the Regulation.
2. Where data relating to the health of persons outside the Court is concerned, ensure that the consent of those persons to process their data has been obtained, in accordance with Article 10(2)(a) of the Regulation; give instructions in that regard to the security firm.

3.3. Data quality

Under Article 4(1)(c) of the Regulation, the data processed must be '*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*'. According to the notification and the information note and in view of the format of the incident report, security staff are able to collect a large amount of data. It is for the Safety and Security Section to remind the processor to process only data that are adequate, relevant and limited to what is strictly necessary in relation to the purposes for which they are collected, namely drawing up reports to enable the Court, where necessary, to take the follow-up action required with regard to security and safety. Therefore, in the majority of cases, the collection of data relating to the health of the data subjects does not seem necessary in relation to that objective.

Recommendation

3. Remind the security firm of the principle of minimising data, in particular with regard to data relating to health.

[13] For example: persons who are injured following an incident with the installations, persons suspected of having sabotaged an installation.

3.4. Data Processor

Pursuant to Article 23 of the Regulation, if a data processing operation is carried out by a processor on behalf of the controller, a contract or legal act must be concluded between the processor and the controller. The contract must stipulate that the processor will act in accordance with the instructions from the controller (so far as the data processing operation is concerned). The processor must ensure compliance with the obligations with regard to confidentiality and security laid down, in the present case, in the national provisions implementing Article 17 of Directive 95/46/EC.

That obligation is met by means of the contracts concluded with the processor.[14] [...]

3.5. Information to be given to the data subjects

Articles 11 and 12 lay down the detailed rules regarding information to be given to data subjects in order to guarantee fair and transparent processing in respect of the data subject.

As regards the **recipients of the data**, the notification and the information note set out a number of potential recipients, including the European Ombudsman and the EDPS. For information, the EDPS notes that authorities receiving personal data in the framework of particular inquiries are not to be regarded as 'recipients' within the meaning of Article 2(g) of the Regulation and must not be mentioned as such in the information note.

As regards the **legal basis of the processing**, it must be amended in accordance with recommendation No 1.

Recommendation

5. Supplement the notification and information note with regard to the legal basis of the processing, in accordance with recommendation No 1.
6. Publish the information note on the website of the Court of Justice.

3.6. Data retention periods

Pursuant to Article 4(1)(e) of the Regulation, personal data must be '*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed*'.

The retention period set out in the notification is ten years. The Court declares that it refers in that regard to general use in the Grand Duchy of Luxembourg regarding the management of safety registers.

That retention period, which is particularly long, has no legal basis and is applied without distinguishing the type of report, the severity of the incident and how the reports are followed up, is disproportionate and does not observe the requirements of Article 4(1)(e) of the Regulation.
Although it may be justified, with regard to general use in the Grand Duchy of Luxembourg, to retain incident reports relating to the safety of installations for ten years, that period does not seem justified, for example, for an incident report recording a collision between two vehicles

[14] Article 16.2. of the contract of 16 November 2010 and Article II.6.1 of the contract of 1 July 2015.

in a Court car park causing only slight material damage or a report on mild discomfort experienced by a visitor to the Court.

The retention period for reports and summaries of the reports should be reassessed by the Court.

Recommendation

7. Reassess the retention period for reports and summaries of the reports, taking particular account of the nature of the reports and how they are followed up.

* *
*

Subject to the reminders and recommendations contained in this opinion, the processing of data by the Court in connection with the management of incident reports appears to comply with the Regulation.

The Court is requested to inform the EDPS of the measures taken to comply with the recommendations of this Opinion within a period of **four months**.

Done at Brussels, 12 September 2016

Wojciech RAFAŁ WIEWIÓROWSKI