Opinion on a notification for prior checking received from the Data Protection Officer of the European Commission related to the "Participatory surveillance research project with evacuation exercise at the JRC/IPSC institute"

Brussels, 05/02/2014 (Case 2012-0824)

1. Proceedings

On 25 September 2012, the European Data Protection Supervisor ("EDPS") received from the Data Protection Officer of the European Commission a notification for prior checking ("the Notification") regarding the data processing operations relating to a participatory surveillance research project with evacuation exercise at the JRC/IPSC institute.

A draft privacy statement was attached to the notification.

Questions were asked to the data controller on 23 October 2012 who replied on 26 October. An additional request was made on 16 November 2012, which was replied to on 9 January 2013. The draft Opinion was sent to the DPO for comments on 17 January 2013. The EDPS sent reminders but neither the Data controller nor the DPO sent any comments.

2. Examination of the matter

2.1. The facts

The notification concerns user data processed within the context of a scientific research by the action "Surveillance Systems and the Citizen" (**SURCIT**) of the Digital Citizen Security unit of the Joint Research Centre (JRC) while investigating participatory surveillance techniques during an evacuation exercise. Participatory surveillance is a novel approach that relies on sensor data from smartphones to contribute to surveillance tasks (e.g. location tracking, identity verification, etc.).

The processing consists of capturing and remote recording smartphone sensor data (location, video, sound, etc.). Participant identification data (name, surname, ID, building, office and photo) are also processed to produce badges and perform ID checks on mobile devices at the meeting point.

The **purpose** of the processing is to study feasibility of the participatory surveillance concept and its legal and technical issues when using latest generation smart mobile devices (smartphones, duplicates of contactless identity cards), such as privacy opt-in/opt-out choices, reliability, efficiency and scalability of the exercise.

The JRC developed and implemented a participatory surveillance test bed. Software and mobile devices (i.e. a dedicated application, 12 test smartphones for end-users (10) and

building delegates (2) and 100 contactless identity cards) will be distributed to a group of volunteer employees with different roles (building delegate, end user) at one of the JRC yearly evacuation exercise. Besides, the experiment will also use a minimum of 20 staff's personal smartphones (meeting specified technical capabilities, e.g. android operating system and available to install a participatory surveillance application for end users).

The procedure can be described as follows:

1. Preparatory registration

The control room maintains a list of mobile phones assigned to users who will participate to the surveillance test with their devices providing various sensing capabilities. The participatory surveillance software is installed in each mobile phone and ready to be used by the building delegate as authenticated user or by staff member as simple end user. The participatory surveillance software[1] limited to the sensor data collection component is distributed to voluntary users wishing to use their personal smartphone for the exercise and consenting to be followed along the evacuation stages.

The control room also maintains the list of staff to be evacuated (i.e. the persons who received the duplicate identity badge required for the participatory surveillance test).

2. Participatory surveillance services for evacuation monitoring

The evacuation alarm will constitute the starting point of the participatory surveillance test and will notify the user of the need for activating the corresponding software on the smartphones, enabling the following services:

- Automatic location tracking
  The location of smartphones involved in the test will be continuously transmitted to the control room and displayed on the map of the evacuation premises (indoor and outdoor area). Additionally the building delegate's contact details will also appear on the map. This function will be available only during the exercise.

- Manual video streaming
  Either on request from the control room or on their own initiative, building delegates will be able to stream short sequences of audio/video content reporting critical events in real-time to the control room.

- Automatic collection of user sensor data
  Throughout all the evacuation procedures, smartphones will capture relevant contextual information that will be uploaded to the control room repository and eventually analysed (speed, battery level, etc.).

- Biometric identity verification of staff members at the meeting point.

[1] A modified version of the open source Funf software made available by MIT, available at: http://code.google.com/p/funf-open-sensing-framework.

Two testing scenarios are planned for performing identity verification using a mobile device:

- In the "badge scenario" a building delegate checks identity of employees at gathering point by reading the information stored in the badge (ID-name, facial image) and taking a picture of the employee. The mobile identity verification application on the mobile terminal matches the two pictures. The matching score is displayed together with a message for final decision. If confirmed, the employee is removed from the list. The ID-name name field is only used to maintain the list of employees.

- A second scenario assumes that an employee at the gathering point does not have a badge with him/her. In this case the building delegate takes a picture of the employee with the mobile identity application whereas the image matching is performed remotely at the control room. Only a few pre-selected users (no more than 10) who would have provided consent to this back-up solution will contribute to this part of the test.

3. End of evacuation exercise

Having received the result of the presence check, the control room can notify the correct execution and conclusion of the exercise. This notification will stop all data collection and finalise their uploading of the server.

4. Post-analysis reporting

The personal data collected in raw format during the exercise will be analysed and aggregated into anonymous statistics (e.g. duration, location, activity).

Personal data on badges and smartphones will be deleted after the exercise execution.
Video recording on smartphone memory card and server repository: video content could be reused for scientific/research publication with granted permission from data subjects. Face will be blurred on the video used for those publications.

As far as **automated/manual operations** are concerned**,** user data are encoded on badges and there is mobile identity verification. Sensor running in background on mobile devices capture environmental data, which are transmitted to the control room server and stored therein. Collected data are then analysed and aggregated in an anonymous way.

According to the notification, the **data subjects** concerned are:

- Building delegates (1 to 2).
- Staff employees from one IPSC building are enrolled for the participatory surveillance project with a smart phone provided to them (10) or with their own smart phone (around 20).
- Staff employees from one IPSC building are enrolled for the participatory surveillance project with a dedicated badge produced for the test (max 100).

The JRC underlined that the participation to the experiment is only made on a voluntary basis.

The **personal data** processed are:
- Biometric/personal data for badges (identifier, name, surname, identity photo, office, building);

- Smartphone user data (android version, battery status, smartphone model, network unique identifier, audio, light, proximity, magnetic field, raw and derived accelerometer values, gravity, orientation, GPS/network location, nearby bluetooth & WiFi devices), including short sequences of video-streams can include images of objects, cars and individuals.

As to the **recipients**, the JRC identifies the following ones:

The Head of Unit representing the JRC as controller of the processing of personal data, the system administrator of the software and the unit staff members from the SURCIT action involved in the research project, i.e. the IPSC/ISM safety and security unit. Safety and security officers might need to check the list of participants to the surveillance test when accessing the result of the study, limited to the following pieces of info: username, location, participant's role, and mobile identity authentication of participants acknowledged by the building delegate.

It is also explained that the data related to the building delegate who is an important actor of the traditional evacuation exercise will be transferred to the safety and security unit only with his explicit consent.

No personal data is transmitted to third parties who are outside the recipients (IPSC SURCIT researchers) and the legal framework mentioned.

Concerning the **rights of the data subjects**, data subject will be offered the opportunity to correct and modify the data they provided and to withdraw their participation at any time by contacting the contact point of the project (a dedicated email and phone number will be available for this point). Moreover, should any data subject withdraw their consent on the use of collected data, the current procedure described in the notification foresees that request for modification would be implemented within one month.

Regarding the **storage** of the data, collected data will be kept on direct access storage of the digital Citizen Security unit lab server, physically disconnected from JRC Internet and not accessible from outside world. From enrolment to evacuation execution, identification data will also be encoded on badges and backed-up on server. As to the security measures of the storage, this is analysed below.

As to the **conservation**, biometric and personal data encoded for badge production will be retained for the time necessary to conduct the experiment and will be deleted within 30 days after the evacuation test.

Smartphone user data and short sequences of video streams will be retained in raw format for the time necessary to perform post-analysis evaluation and technique validation of location tracking, quality assessment of video content (1 year).

As regards the **information** provided to the data subject, at recruitment data subjects will be informed about the processing of their data in the framework of the experiment by a privacy statement (the draft of the privacy statement has been sent to the EDPS as part of the documentation).

Security measures

A security requirement analysis was carried out in consultation with the JRC Local Informatics Security Officer. As an outcome, no security plan was produced. Yet different security measures have been designed and implemented:

[...]

2.2. Legal aspects

2.2.1. Prior checking

This prior checking Opinion relates to the processing of personal data by the JRC, carried out within the context of a scientific research by the SURCIT action of the Digital Citizen Security unit of the JRC while investigating participatory surveillance techniques during an evacuation exercise.

Applicability of the Regulation. The notification concerns the processing of personal data, within the meaning of Regulation (EC) No 45/2001. The data processing is performed by a European Union body, the European Commission (Directorate General JRC), in the exercise of activities which fall within the scope of EU law[2]. Personal data of individuals which are directly identifiable (Article 2(a)) will be processed in order to analyse how and if the individual can participate and contribute to the description of a situation. For the evacuation exercise scenario selected, the JRC is exploring the technological capabilities of the smartphone platform for contributing to the resolution of the event and its different steps.

These activities constitute partially automated and partially manual processing operations. The processing therefore falls within the scope of Regulation (EC) No 45/2001.

For the reasons described above, all elements that trigger the application of the Regulation are present:

Grounds for prior checking. Article 27(1) of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS *"processing operations likely to present specific risks to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes"*. The EDPS considers that the presence of some biometric data other than the simple storage of photographs alone, such as the case in point where biometric matching is taking place, presents specific risks to the rights and freedoms of data subjects[3]. These views are mainly based on the matching process of biometric data and on the nature of biometric data which is highly sensitive, due to some inherent characteristics of this type of data. For example, biometric data changes irrevocably the relation between body and identity, in that they make the characteristics of the human body 'machine-readable' and subject to further use. In this case, biometric matching system will be used for a research activity. Although the processing operation is taking place within the framework of a research activity aiming at contributing to the improvement of the efficiency of future applications regarding privacy, data protection

[2] The concepts of "Community institutions and bodies" and "Community law" can not be any longer used after the entry into force of the Lisbon Treaty on 1st December 2009. Article 3 of Regulation 45/2001 must therefore be read in light of the Lisbon Treaty.

[3] See also case 2007-0501 (Iris scan system at the European Central Bank) and case 2007-0635 (Access control at OLAF).

and security, the risks described above justify the need for the data processing itself to be prior checked by the EDPS in order to verify that stringent safeguards have been implemented.

The EDPS understands that the notification relates only to processing operations in the context of a project conducted by SURCIT and that no real implementation is planned within the JRC or the European Commission. However, should such situation be envisaged, the European Commission would need to submit the processing operation for PC again.

Prior Checking. Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this present case, the notification relates to a processing which has not yet taken place at the JRC and therefore qualifies for **prior-checking.**

Notification and due date for the EDPS Opinion. The notification was received on 25 September 2012.

Pursuant to Article 27(4) of Regulation (EC) No 45/2001, the two-month period within which the EDPS must deliver an Opinion was suspended for a total of 412 days (26 days of suspension to obtain additional information plus 386 days allow comments on the draft Opinion.

2.2.2. Lawfulness of the processing

Personal data may only be processed if legal grounds can be found in Article 5 of Regulation (EC) No 45/2001. The notification points out that the grounds that justify the processing operations are based on Article 5(a) and Article 5(d). Pursuant to Article 5(a) personal data may be processed if the processing is "*necessary for the 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 interpreting Article 5(a), recital 27 states that: "*processing of personal data for performance of tasks carried out in the public interest includes the processing necessary for the management and functioning of those institutions and bodies*".

In this case, the processing at stake cannot be considered as necessary for the management and functioning of the JRC itself, as described in Recital 27. However, it can be based on other public interests as stated in the Framework 7 Research Programme under which the JRC provides technical and scientific support to EU policy development[4]. In this respect, the EDPS considers that the necessity of the processing could be considered as justified.

Moreover, under Article 5(d), personal data may be processed only if the data subject has unambiguously given his or her consent. As stated in the notification, the data collection of building delegates and end users is organised on a voluntary basis and the transfer of data of building delegates is performed only with their explicit consent. Given the employment relationship at stake, specific safeguards must be put in place in order to ensure that consent is authentic and freely given. In particular, before asking for consent the controller must not only provide complete information about the purposes but also on all the relevant elements of the procedure and inform the data subject that adhesion to the test is fully voluntary and that

[4] Council Decision 2006/975/EC of 19 December 2006 concerning the Specific Programme to be carried out by means of direct actions by the Joint Research Centre under the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007 to 2013).

there will be no consequences in case of refusal. The controller should furthermore exercise no pressure on the data subjects' decision. The information should be provided and the consent should preferably requested in writing by e-mail.

2.2.3. Data quality

Adequacy, relevance and proportionality. Pursuant to Article 4(1)(c) of Regulation (EC) No 45/2001, personal data must be adequate, 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.

In analyzing whether the processing in point, which involves the processing of user data (including biometric and smartphone user data) is in line with this principle, the EDPS concludes on the basis of the information provided by the controller that the data collected could be considered adequate and relevant for the purposes of the processing. Biometric/personal data for badges (identifier, name, surname, identity photo, office, building) and smartphone user data are processed solely for the purpose describe.

However, regarding the application that is installed in the smartphones of the data subjects themselves, the EDPS has not received information as to the deletion of this application at the end of the experiment. As to ensure that the system does not track data subjects after the period foreseen in the notification nor that tracking would take place outside the perimeter where the experiment is conducted, the EDPS recommends that controller ensures that the application will be deleted from the smartphones of the data subjects at the end of the test, therefore avoiding further potential tracking.

Fairness and lawfulness. Article 4(1)(a) of the Regulation requires that data be processed fairly and lawfully. The issue of lawfulness was analyzed above (see Section 2.2.2). The issue of fairness is closely related to what information is provided to the data subjects and is further addressed in Section 2.2.7.

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 accuracy of the data is ensured as the data subject is offered the opportunity to correct and modify the data they provided. Furthermore, the security measures put in place and the additional ones recommended in the present Opinion may also contribute to reinforce the accuracy of data processed. This is also foreseen in the privacy statement which was provided.

2.2.4. Conservation of data

Pursuant to Article 4(1)(e) of Regulation (EC) No 45/2001 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. This is usually referred to as the 'conservation principle'.

As stated in the facts, there are two retention periods linked to the end of lifecycle of the processing:

- biometric and personal data encoded for badge production will be deleted within 30 days after the evacuation test,
- smartphone user data and short sequences of video streams will be retained in raw format for the time necessary to perform post-analysis evaluation and data quality assessment (1 year).

The EDPS takes note of the respective retention periods and considers them adequate to the purpose of the processing. In the case that the JRC wants to keep the data for a longer period than originally planned, the JRC shall contact the EDPS and justify this request.

2.2.5. Transfers of data

Only transfers under Article 7 of the Regulation shall apply in this case as the data are only transferred within a European institution (the JRC of the European Commission) to specific users within this institution. In this context, the EDPS considers that such transfer is necessary for the legitimate performance of tasks covered by the competence of the respective recipients, as provided by Article 7(1) of the Regulation.

2.2.6. Right of access and rectification

According to Article 13 of Regulation (EC) No 45/2001, 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*". Article 14 of the Regulation provides the data subject with the right to rectify inaccurate or incomplete data.

The rights of access and rectification are provided to the data subject and this is also stated in the privacy statement provided.

However, as the participation into the scheme is linked to the consent of the data subject, this consent may be revoked. The EDPS notes that the notification foresees that should any data subject withdraw their consent on the use of collected data, request modification will be made within one month. In the light of the length of the processing notified and the use of data being done, the EDPS suggests modifying this time limit to 15 days maximum instead of the current planned retention of one month.

Moreover, the notification also states that a dedicated email and phone number will be available for withdrawal of consent. However, although the phone number does not seem to be foreseen in the draft privacy statement that was provided with the notification, the EDPS would in any case rather favour a system using only email contact as a medium of proof of the request to withdraw the consent. The JRC should adapt this information in its notification.

2.2.7. Information to the data subject

Pursuant to Articles 11 and 12 of Regulation (EC) No 45/2001, 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.

The EDPS received the draft of the privacy statement that contains the elements listed under Articles 11 and 12 and therefore concludes that these articles are complied with. The EDPS understands that the data controller has informed the data subjects that the tracking system requires activation by the user, and cannot be activated without the latter's involvement (e.g. by the administrator).

2.2.8. Security measures

According to Articles 22 and 23 of Regulation (EC) No 45/2001, the controller and the processor must implement appropriate technical and organizational 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 unauthorized disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing.

The processing is subject to the Commission Decision C(2006) 3602 of 16 August 2006 concerning the security of information systems used by the European Commission (EC) adopted on 29 May 2009 (hereinafter the Decision). The EDPS considers this Decision, as detailed by its implementing rules (IR) and security standards, as a sufficient base for respecting Article 22 of the Regulation.

[...]

3. Conclusion

The proposed processing operation would not appear to involve any breach of the provisions of Regulation (EC) No 45/2001, provided that account is taken of the observations made above. In particular, the JRC should:

- ensure the respect of the informed consent of the data subjects by providing all the relevant elements of the processing operation and ensure that the consent is provided in writing;

- review the proposed period to implement the deletion of data after the withdrawal of the consent by a data subject;

- foresee that the request for withdrawal of consent is provided in writing;

- foresee the removal of the installed application from the smartphones of the data subjects at the end of the exercise;

[...]

(**signed**)

Giovanni BUTTARELLI