Opinion on a notification for prior checking received from the Data Protection Officer (DPO) of the European Parliament in connection with the 'Biometric verification device' case

1. Proceedings

On 9 October 2013, the European Data Protection Supervisor (**EDPS**) received from the Data Protection Officer (**DPO**) of the European Parliament (**the Parliament**) a notification for prior checking relating to the processing of personal data in the context of the Parliament's biometric verification device.

The EDPS also received a number of documents relating to that notification, namely:

1. Decision of the Bureau of the Parliament on the global security concept;
2. Decision of the Bureau on bringing the Parliament's security under internal management;
3. Confidentiality declaration relating to the biometric verification device.

In addition, on 21 October 2013, the EDPS received more detailed technical information relating to the biometric system chosen by the Parliament and also replies to a series of technical questions which had been asked. The deadline for delivery of the opinion by the EDPS was then extended by two months on 9 December 2013 on account of the complexity of the facts, in accordance with Article 27(4) of the Regulation. On 10 January 2014, the deadline was suspended with a view to a meeting being held with the Parliament. The meeting took place on 30 January 2014. Following that meeting, a new set of questions was sent to the Parliament. The Parliament replied to those questions on 26 March 2014.

The notification was submitted for prior checking under Article 27(1) of Regulation (EC) No 45/2001 ('the Regulation').

2. The facts

Following the decision to bring its security under internal management, the Parliament decided to reuse an existing biometric verification device in order to ensure that security posts are occupied only by prevention and security officers and by authorised security staff.

That biometric system is currently used by the external company in charge of the Parliament's security (Securitas). As a result of the decision to bring security under internal management, the Parliament will in the future employ prevention and security officers reporting directly to its own authorised official and security guards reporting to an external provider for specific needs ... According to the notification, the choice of solution follows the draft global security concept adopted by the institution. The Directorate for Resources, and in particular the departments responsible for planning and the control centre, are responsible in practice for the implementation of the processing operation. Enrolment of officers in the system is carried out by the planning department for EP officers and by Securitas for Securitas officers …

The Parliament has taken the view that the installation of such a device is essential in order to respond to the security needs with which it is faced. Those security needs cover, in particular, management of the prevention and security officers responsible for the Parliament's many physical access points. The Parliament must be able to verify the identity of officers on duty in order to prevent fraudulent practices in the manning of security posts. It is necessary:
- to prevent the Parliament's internal prevention and security officers from swapping their posts with guards reporting to the external provider and vice-versa, for reasons of security and liability, particularly in the event of an accident;
- to prevent certain officers, in agreement with others (the officer preceding or following them at the same post), from failing to adhere to their specified working hours, thereby increasing the level of security risk;
- to ensure that officers actually occupy the post which they are **authorised to occupy**. The following are mentioned by way of examples: (i) officers assigned to posts at the crèches managed by the Parliament, who must have undergone specific training and must provide a special extract from the judicial record; (ii) officers at posts connected with the operation of metal detector gates and X-ray machines, who must also have undergone specific training; (iii) … ; (iv) officers at posts at entrances to car parks, who require specific equipment; and (v) account must be taken of individual bars on medical grounds, which must be respected.

According to the Parliament, such a need therefore means that it must be possible for the department in charge of planning to be informed about, and to have effective and reliable control of, the manning of posts, so that it can take action in the event of absence or fraudulent practices in the manning of posts, which could lead to unlawful access to the institution's security instructions (for example …).

As regards the system's operating principle, the biometric reader captures a three-dimensional image of the hand. After the image is captured, the reader converts the image into an electronic template. That template and the associated user's identification number are stored in databases which, in the event ...

In the planned procedure within the Parliament, the department in charge of planning prescribes the assignment of officers. When starting/finishing his/her shift, an officer must present his/her badge and his/her hand in order to identify him/herself. The user uses a badge reader integrated into the biometric reader to capture his/her identification number. Next, the biometric reader invites the user to place his/her hand on the scanner. The reader then compares the hand placed with the unique template stored …

Consequently, the biometric characteristics and the identifier (badge) (…), on the one hand, are matched with the identifier, staff number, surname and first name of the officer … on the other.

The **data subjects** are the security officers employed by the Parliament and Securitas. The enrolment procedure is dealt with by managerial staff.

The **data collected** in the course of the processing operation are:
- surname and first name;
- biometric template (corresponding to biometric characteristics converted into digital form according to a specific standard/coding) and not raw biometric data;
- the officer's identifier (badge);
- the staff number;
- data relating to shift start and finish times.

As regards t**he recipients of the data** processed, the data relating to hours worked will be transferred to the competent departments of the DG PERS (transfer made from the Planning database to the Streamline database):

- individual rights and remuneration;
- staff management and careers (impact of extended leave on career).

It is also stated that, where applicable, data are transferred to the department which manages medical absences.

…

As regards biometric data … These biometric data are not transferred to the planning department, which receives only data relating to the officer's identifier and shift start and finish times, which it verifies and validates.

As regards the **rights of data subjects**, the notification stipulates that data subjects may exercise their rights of access, rectification, blocking, erasure and objection at any time by sending a request to the planning department …

Furthermore, as regards the rights of data subjects, the controller must give a decision within 15 working days of receipt of a request for blocking. If the request is accepted, it must be carried out within 30 working days and the data subject must be informed about it. Where a request for blocking is refused, the controller has 15 working days to notify the data subject by letter, stating reasons.

Similarly, the controller must reply within 15 working days of receipt of a request for erasure. If the request is accepted, it must be carried out without delay. If the controller considers the request to be unjustified, he/she has a period of 15 working days in which to inform the data subject of this by letter, stating reasons.

According to the notification, **information** is to be provided to data subjects by means of:
- training for newly recruited officers, in which the Parliament's Data Protection Officer will take part;
- a declaration on data protection, including all the characteristics of the processing in question, as required by Articles 11 and 12 of the Regulation. The Parliament has provided a draft confidentiality declaration.

As regards **the retention of data**, the notification stipulates …

In relation to the **data retention period**, according to the procedure currently planned:
Data relating to officers' identity, the identifier (badge) and the biometric characteristics will be retained … for the period during which the officer is required to perform duties as a prevention and security officer – security tasks and duties.

Regarding the **technical and security features** of the biometric system, the controller has supplied additional information regarding the structure and description of the system chosen:

these consist primarily of: …

3. Legal analysis

3.1. Prior checking

Applicability of the Regulation: this opinion relating to prior checking concerns the processing of personal data by the European Parliament.

The Regulation applies to the '*processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system*' and to the processing of personal data '*by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law*.' For the reasons set out above, all the elements giving rise to the application of the Regulation are present.

First, *personal data*, as defined in Article 2(a) of the Regulation, are collected and further processed. Next, the personal data collected are '*processed by automatic means*', within the meaning of Article 2(b) of the Regulation. Personal data such as personal identification data, including handprints, are collected and 'processed by automatic means', for example when the service takes the prints. Lastly, the processing is carried out by an institution, in the present case the Parliament, in the exercise of activities which fall within the scope of EU law (Article 3(1) of the Regulation).

Ground for prior checking: Article 27(1) of the Regulation makes subject to prior checking by the EDPS '*[p]rocessing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*'. The EDPS believes[1] that the existence and processing of biometric data other than photographs, as occurs in the present case given that biometric handprints are collected, may present particular risks to the rights and freedoms of the data subjects. He draws that conclusion essentially from the nature of biometric data, because of the inherent characteristics of that type of data. For example, biometric data make the characteristics of the human body 'machine-readable' and liable to be put to subsequent use. Those risks may justify the need to make the data processing operation subject to prior checking by the EDPS under Article 27(1) of the Regulation in order to confirm whether strict guarantees have been implemented.

In addition, the EDPS believes that, in certain cases, the integration of RFID technology (card with RFID chip integrated into the badge) may lead to specific risks. In the present case, the use of RFID technology is planned only for the badge which, currently, does not contain any biometrics. According to the information received, the Parliament envisages, however … In this case, the EDPS wishes to point out that that could lead to a change in the risks presented by the processing.

Deadlines: Since the aim of the prior checking is to address situations likely to present specific risks, the opinion of the EDPS must be delivered before the start of the processing operation, in accordance with Article 27 of the Regulation. Therefore, the processing operation must not be implemented until such time as the EDPS gives his formal approval.

The notification was received on 9 October 2013. Under Article 27(4) of the Regulation, the EDPS must deliver his opinion within two months (in the present case, the procedure was

[1] See also cases 2010-0427 of 8 September 2011, 2007-635 of 7 April 2008 and 2008-223 of 30 June 2008, available on the EDPS website.

suspended for a total of 75 days in order to obtain additional information, and a further 20 days were added to that period in order to enable the submission of comments on the draft opinion). Therefore, the present opinion must be adopted by 15 May 2014 at the latest.

3.2. Lawfulness of processing

Processing of personal data is permitted only if it is based on Article 5 of the Regulation. Among the various grounds laid down in Article 5 of the Regulation, Article 5(a) appears to apply to the processing operation notified. In accordance with that provision, personal data may be processed only if it 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 order to determine whether the processing operation complies with Article 5(a) of the Regulation, three elements must be taken into account: first, whether the Treaties or other legislative acts provide for the processing operation carried out; second, whether processing is carried out in the public interest; and third, whether processing is actually necessary for the performance of a task carried out in the public interest (necessity test). The three requirements are closely linked.

* The **legal basis** applicable to the processing operation in question is described in the following acts:

- Decision of the Bureau of 6 July 2011 on the global security concept;
- Decision of the Bureau of 11 June 2012 on bringing the Parliament's security under internal management.

Those decisions make provision for the development, within the Parliament, of a 'global security concept' and for management of the Parliament's security to be brought gradually under internal management.

Decisions of the Bureau of the Parliament are provided for in the Parliament's Rules of Procedure, adopted under Article 232 of the Treaty on the Functioning of the European Union.

Processing is carried out in **the legitimate exercise of official authority**. The EDPS observes that the Parliament performs the processing operations in the context of a task carried out in the legitimate exercise of its official authority on the basis of the above-mentioned legislative acts adopted on the basis of the staff regulations. The Parliament has adopted a global security concept of which the processing operation notified forms part.

As regards the need for the processing **(necessity test)**, in accordance with Article 5(a) of the Regulation, data processing must be '*necessary for the performance of a task*', as mentioned above. In that connection, recital 27 in the preamble to the Regulation states that '*[p]rocessing of personal data for the performance of tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies.*'

The need put forward by the Parliament for the use of the biometric verification system is based on general security needs, which include the specific management of its security staff (addressing any non-compliances by its staff, such as fraudulent practices in the manning of posts). However, the EDPS cannot lose sight of the fact that the choice of the specific

technical solution (including biometric hand recognition) is also linked to the fact that that solution is currently used by the external security company contracted to the Parliament (Securitas). Even if that is not the main factor leading to the final decision to use that solution, it is a factor which cannot be disregarded in the current analysis.

It is therefore difficult to establish the absolute need to implement the specific biometric system chosen by the Parliament rather than another system. Thus, 'necessity' must not be considered to mean that the process is inevitable, but rather that it may be regarded as reasonably necessary in the specific context of the objective it is desired to achieve. It appears that, in the limited context of the management of prevention and security staff – which has a direct effect on the security of the Parliament in general – the processing operation may be regarded as reasonably necessary. It should be recalled that the ultimate aim of the processing operation is the physical protection of the institution's staff, information and property.

In view of the importance of those interests, the Parliament may in fact consider it necessary to adopt special security measures, in particular the implementation of rigorous systems for checking the identities of members of the security team, giving rise to the personal data processing operation in question.

The implementation of that specific biometric system and that … appear to be appropriate measures for limiting fraudulent practices in the manning of posts.

Nevertheless, the EDPS notes that, at the present time, the verification procedure consists essentially of a verification process …

The EDPS considers that system to be less respectful of private life than a system in which the verification procedure consists of a 1:1 verification process within the badge (one to one) – in which the details are included in the holder's card and compared with the details scanned (for verification purposes) on the spot, with the aid of a biometric data reader/scanner. Comparison/verification would be carried out locally by the biometric data reader … The EDPS is in favour of that system, which prevents any subsequent unlawful use and 'phishing attacks', which are generally the consequence of the use of databases[2].

Based on his consistent approach to biometric data processing[3], the EDPS is unable to fully support the approach taken by the Parliament while the system currently used remains in its present form. Although the Parliament has announced its intention to migrate the current system to that second 1:1 verification system, there is, at the moment, no precise timetable for such a migration. The EDPS therefore asks the Parliament to make every effort to carry out that migration in accordance with a precise timetable to be supplied.

3.3. Data quality

Adequacy, relevance and proportionality: under Article 4(1)(c) of the Regulation, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. That is the principle of data quality.

With regard to biometric data, the EDPS notes that the system is based on a biometric hand contour template.

[2] See the opinion on a notification for prior checking received from the data protection officer of the European Central Bank, concerning the incorporation of iris scanning technology into a pre-existing access control system for highly secured areas of the ECB, 14 February 2008 (2007-501), available on the EDPS website.
[3] See footnote 1.

The type of data collected, the biometric characteristics of the hand and related identity information, correspond to the data required for operation of the system based on biometric data. From that point of view, the EDPS observes that the data collected could be regarded as adequate and relevant for the purposes of the processing operation.

Fairness and lawfulness: Article 4(1)(a) of the Regulation provides that data must be processed fairly and lawfully. The question of lawfulness was analysed above (see point 3.2), while the question of fairness is closely linked to that concerning the information to be provided to data subjects, which is dealt with below at point 3.9.

Accuracy: according to Article 4(1)(d) of the Regulation, personal data must be '*accurate and, where necessary, kept up to date; 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 the present case, the personal data affected by the processing operation consist of biometric data used for the purpose of identity checking. Certain key features of biometric systems have a direct effect on the level of accuracy of data generated during the enrolment and identification stages inherent in that type of system. Depending on whether or not the biometric system has been set up in a way which incorporates those key elements, the accuracy of the data will (or will not) be a parameter to be considered.

In previous opinions relating to access control systems, the EDPS has analysed the rules to be followed when implementing biometric systems. The following analysis describes the key elements and evaluates the extent to which those elements have been taken into consideration in relation to the Parliament's biometric verification device.

Firstly, any enrolment stage must make provision for alternative means of identification for persons who are not eligible, even temporarily, for the enrolment procedure, for example as a result of damaged handprints. That procedure is generally described as a '***fallback procedure***'[4]. In the case of enrolment, the terminal validates or refuses enrolment and refusal occurs where the enrolment is of poor quality etc.

Next, at the stage where the technology is used, biometric verification may also not be possible. The EDPS notes that it is planned to implement such a fallback solution where biometric verification is impossible (the notification uses the term 'system error'). In such a case …

The EDPS also notes that another measure, aimed at ensuring the accuracy of data, is applied by the technology used. If a person does not use the devices regularly, the data collected at the time of verification will no longer match the data stored. That is explained by the fact that human hands change naturally (weight gain or loss, joints changing with age, etc.). To prevent that problem, every time a measurement/verification is effected, an average measurement is automatically created and stored on the device as fresh data; the previous data are replaced by the new, fresh data.

The EDPS considers those fallback procedures to be sufficient in the light of Article 4(1)(a).

[4] For a description of the data protection principles applicable to fallback procedures, see the Opinion of the European Data Protection Supervisor on the draft Council Regulation (EC) laying down the form of the laissez-passer to be issued to members and servants of the institutions (OJ 2006 C 313, p. 36).

3.4. Data retention

Under 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.

As regards the retention period currently planned … the EDPS notes that the period stipulated for the different categories of data related to identification and biometric characteristics could be regarded as justified.

However, in view of the comments already made … the retention period … must be reviewed in order to set an appropriate retention period ...

3.5. Transfer of data

Transfers are planned under Article 7 of the Regulation. The EDPS observes that Article 7 of the Regulation permits transfers of personal data if those data are '*necessary for the legitimate performance of tasks covered by the competence of the recipient*'. For the purpose of compliance with that provision, where personal data are transferred, the controller must ensure that (i) the recipient has the appropriate competence and (ii) the transfer is necessary. The EDPS believes that those conditions are satisfied in the present case.

The data relating to hours worked will be transferred from the planning department to other competent departments of the DG PERS, namely the 'individual rights and remuneration' department and the 'staff and career management' department. Those transfers will be from the Planning database to the Streamline database. Where applicable, the data are transferred to the department responsible for dealing with absences on medical grounds. Those recipients must process the data for the purposes for which the data are sent to them, in accordance with Article 7 of the Regulation.

3.6. Processing of personal number or unique identifier

Article 10(6) of the Regulation provides that '*[t]he European Data Protection Supervisor shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body*.' This Opinion will not stipulate the general conditions for use of a personal number, but will consider the specific measures necessary in the context of biometric verification within the Parliament.

In a previous opinion on prior checking[5], the EDPS has already explained the status of a chip-card number incorporated into a card. The identification number associated with an RFID chip card is included in the personal data covered by Regulation No 45/2001. Where such an identification number is used to assess the conduct of a staff member and is linked to the personal number (to the name of a person, as occurs in the present case), it gives rise to the processing of personal data, and therefore necessitates compliance with the principles of data protection.

Use of the personal number is necessary because the card identifier is communicated to the biometric control system. In the present case, the use of the personal numbers of staff members for the purpose of verification of data relating to the right of access in the system is

[5] See the Opinion on a notification for prior checking received from the data protection officer of the European Commission concerning the 'implementation of Flexitime specific to the DG INFSO', 19 October 2007 (2007-218).

reasonable if the number is deemed to be used to identify the person concerned in the system and thus makes it possible to ensure the accuracy of the data. There is no reason to establish any other conditions in the present case.

3.7. Rights of access and rectification

In accordance with Article 13 of the Regulation, '*[t]he 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 of any available information as to their source'*. Article 14 guarantees that data subjects have the right to rectify inaccurate or incomplete data.

The notification and confidentiality declaration contain that information (see point 2 'the facts' above). Furthermore, the notification also sets out the policy for blocking/erasure of data following a legitimate, reasoned request from data subjects.

In cases where Article 20 is applicable (for example, in the case of an enquiry), the EDPS points out to the Parliament that it should be applied strictly and on a case-by-case basis.

In conclusion, the EDPS believes that the conditions laid down in Articles 13 and 14 of the Regulation are satisfied, while Article 20 of the Regulation should be applied on a case-by-case basis.

3.8. Information to be supplied to data subjects

Under Articles 11 and 12 of the Regulation, controllers must inform data subjects that their personal data have been collected. In addition, data subjects are entitled to be informed, in particular, about the purposes of the processing operation, the recipients of the data, and their specific rights as data subjects.

The Parliament has sent the EDPS a draft confidentiality declaration intended for data subjects (officers) who will use the biometric verification system. However, the Parliament has not explained when and how that declaration will be made available to data subjects.

The information will also be provided by means of training for newly recruited officers, in which the Parliament's DPO will take part.

Regarding the confidentiality declaration, the EDPS has also examined the content of the information supplied in order to verify whether it meets the requirements of Articles 11 and 12 of the Regulation. The EDPS notes that the data relating to hours worked and absences on medical grounds are transferred to the 'individual rights and remuneration', 'staff and career management' and 'medical absence management' departments, as applicable (see point 3.5). Those three departments are therefore data recipients who are important to the data subjects. In order to ensure fair data processing, the confidentiality declaration should state which data each department is to receive and for what purposes.

If follows that that information on the source of the data processed in the context of the connected processing operations referred to above must also appear in the relevant confidentiality declarations (management of hours worked, management of leave, management of absences on medical grounds, etc.). The relevant notifications must be updated as appropriate.

3.9. Security

In accordance with Article 22 of the Regulation, the controller must implement appropriate technical and organisational 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.

In the present case, as pointed out above, the choice of specific solution is also linked to the fact that that solution is currently used by the external security company contracted to the Parliament. In view of the changes in responsibilities, it would be appropriate for the Parliament to review the risk analysis so as to determine which controls should be put in place in order to reduce the risks to an acceptable level for the Parliament.

…

Furthermore, the EDPS draws the Parliament's attention to the following technical considerations …:

…

Conclusion

The proposed processing operation does not appear to entail any infringements of the provisions of Regulation (EC) No 45/2001, provided that account is taken of the recommendations made above. This means, in particular, that the Parliament should:

- make every effort to modify the current system … and to provide the EDPS with a timetable for those modifications;
- provide clear information to the staff concerned about the recipients of the different categories of personal data and update the information given to data subjects in the context of the connected processing operations (see point 3.8);
- inform the EDPS about how and when the confidentiality declaration will be provided to the data subjects.

Further, as regards the security aspects of the solution, the EDPS recommends that the Parliament:

- …

Finally, as regards the transfer of data to Securitas, the EDPS recommends that the Parliament:

- …

Done at Brussels, 15 May 2014