From: [redacted]

To: [redacted]

CC: Data Protection EP <Data-Protection@europarl.europa.eu>; HAROU Delphine <delphine.harou@edps.europa.eu>; [redacted] European Data Protection Supervisor <EDPS@edps.europa.eu>

Sent at: 19/06/18 17:05:01

Subject: EDPS informal comments: EDPS case 2018-0553 - Reply to "Strictly Confidential: Nouveau dossier qui nécessite une discussion"

Dear [redacted],

Thank you for your e-mail of 18 June, whereby you asked EDPS first advise -by 19 June- on the project "Facilitation de la signature du Registre Central d'Emargement par digitalisation".

Please note that we have filed this message as request for informal consultation pursuant to Article 46(d) of Regulation (EC) No 45/2001 (the Regulation) under EDPS case number 2018-0553.
This means that the first indications by EDPS concerning the project at stake (hence, "the project") we are providing you as a reply to your email are given as staff level reply, not involving the EDPS Supervisors. This is also due to the extreme brevity of the timeframe for this (informal) consultation.

On the content, with regard to the project, as preliminary reply, we note as follows:
▪ From the document "Frequently asked questions" (hence FAQs) attached to the e-mail dated 6 June 2018 from [redacted] to you as [redacted] and having as Subject "Bureau Note – Signing of central register", we note that the EP envisages the use of a biometric (fingerprint) reader for the registration of the presence of Members of Parliament (MEPs).

This 'automated registration system' would work as follows: "when a person is first enrolled in a biometric time and attendance system, the biometric reader records an image of the fingerprint (initialisation phase). The image is stored as a template associated with his/her MEP identification number. Each time the MEP places the finger in the biometric scanner, the reader verifies that the newly scanned image matches the template originally stored for his/her identification number. If there is a match, the attendance is recorded."
Concerning the storage of the biometric template, the FAQs, at question 5, specify that: "a biometric template is generated after post-processing the image, which is stored in a database [...]. This biometric template is just a mathematical representation of the scanned print, i.e. a sequence of binary data. It is nearly impossible to recreate print image with this data. These safeguards make print data storage secure even if a data breach occurred" and at question 10 the FAQ specify that "the registered templates are stored in the respective readers and on a central server during the test phase."
In this regard, I take note that you clarified orally to me yesterday that in the implementation phase (that is, following the test phase) the templates will only be stored in the respective readers.

I also take note that the main driver for the implementation of the project (the new biometric registration system) is financial savings (as you specified to me orally yesterday): namely, as pointed out in the "Note à l'attention des membres du Bureau D(2017)15113": "optimiser l'utilisation des ressources humaines [...] correspondant à environ 170.000 EUR du budget des agents contractuels sur base annuelle".

Finally, I note that the introduction of the new biometric registration system requires an amendments to art. 12 of the "Mesures d'application du Statut des Députés (MAS)". The afore said "Note à l'attention des membres du Bureau D(2017)15113" contains -as attached document- the proposed modification: addition to art. 12.1 of the wording: "Un relevé informatisé de la présence du député peut remplacer la signature personelle".

▪ Against this background, we recall that the EDPS has considered (in case 2014-0496, see attached opinion) the use of a biometric-based system for working time control as not necessary, and therefore not legitimate pursuant to Article 5 of the Regulation ("the requirement of the processing of personal data being necessary in relation to the purpose obliges the controller to assess whether the purpose of the processing could be achieved with less intrusive means. Indeed, instead of opting for a system using biometric data, other systems should have been considered by (...) in this context, such as: signing in, using attendance sheets, or using clocking in systems via magnetic badges.")

In other words, the processing of personal data by an EUI shall be in compliance with Article 5(a) of the Regulation, according to which: "personal data may be processed only if 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 or in the legitimate exercise of official authority vested in the Community institutions or body or in a third party to whom the data are disclosed". Hence the necessity (of the data processing) needs to be proven by the controller (in this case, the EP) as a pre-requisite to the processing.
Regarding the MEPs' presence registration, the EDPS considers that the use of fingerprints-based system for the monitoring of MEPs presence (not for security purposes, but for the purpose of checking eligibility to allowances) is not necessary and, therefore, the envisaged processing of personal data would be in breach of aforesaid Article 5.
We note that the same purpose can be achieved by less intrusive means, such as:
- a PIN code;
- signing attendance sheets;
- clocking-in systems via magnetic bands;
- two-factor authentication, by the combination of more than one of the abovementioned solutions;
- random and periodic checks of the signatures/presences by human monitoring.

The necessity of a fingerprints-based systems for the monitoring of attendance aiming at fraud prevention (taking into account that there are many alternative ways of assessing the effective presence of the MEPs) has not been duly substantiated by the EP. For this reason, the EP should not start the test/pilot phase for the full implementation of the project.

Please note that only in very specific and exceptional cases, related to security, the EDPS has so far considered the use of biometric data, subject to a number of conditions and safeguards, as being in line with the Regulation [see EDPS Opinion of 30 June 2008 on a notification for prior checking on CBIS identity and access management system (Case 2008-223) relating to processing of personal information carried out by OLAF, in particular the Information Services Division, to ensure that only authorized persons have access to OLAF's core IT systems and to allow investigation of security incidents. The Opinion is also attached to this reply email].
Please also note that so far, in the aforesaid specific and exceptional cases, the EDPS has always preferred "1:1 only identification systems", meaning identification systems with no central storage at all (technically: the fingerprint template is stored on the badge; the reader compares the scan to the template on the badge; there is no storage of all prints in the reader or anywhere else). Contrary to this system, it appears from the documentation provided that the EP envisages a "1:n" identification system, with all templates stored in the readers.
We consider that the fingerprints-based system should not be used at all (since the necessity for this processing has not been demonstrated by the EP) and that if (under an 'alternative reality' scenario) that necessity had been demonstrated by the EP, then the identification system should however be "1:1" instead of "1:n".

For the sake for clarity, we reiterate that the project does not meet the 'necessity test' under Article 5(a) of the Regulation, and we add that -again under an 'alternative reality' scenario (that is, if the necessity test is fulfilled)- the processing of biometric data should follow and take into account the outcome of a data protection risk assessment (DPIA). The performance of such DPIA is a legal obligation for the controller under the proposal for new regulation

45 that aligns the regulation to the GDPR. In this regard, we also point out that under the GDPR 'biometric data', as defined at (15) of Art. 4, are considered as personal data to which specific (higher level of) protection applies (see, among others, art. 9 of the GDPR).

▪ Finally, we note that in any case - again without prejudice to our consideration that the project does not meet the 'necessity test' under Article 5(a) of the Regulation - the amendment to art. 12.1 of the Mesures d'application du Statut des Députés (MAS), referring to the "relevé informatisé de la présence" does not contain a reference to the processing of biometric data and therefore it would not be sufficient to provide a legal basis to the 'project', and we also point out, as key requirement, to the obligation on the EP as controller to inform the data subjects about the processing pursuant to art. 11 of the Regulation.

We hope that this information, provided as preliminary informal reply, is helpful.
Please do not hesitate to contact me for any queries in this regard.

Best regards,
[redacted]

Legal Officer
Supervision and Enforcement Unit
European Data Protection Supervisor (EDPS)
[redacted]
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels

-----Original Message-----
From: [redacted]
Sent: 18 June 2018 11:12
To: [redacted]
Cc: Data Protection EP <Data-Protection@europarl.europa.eu>; HAROU Delphine <delphine.harou@edps.europa.eu>
Subject: Strictly Confidential: Nouveau dossier qui nécessite une discussion
Importance: High
Sensitivity: Confidential

Dear [redacted],

As discussed, please, find in attachment the documentation I have received on the file.
Please, consider it as strictly confidential.

I would like to discuss with you your first feeling by tomorrow, if possible, in view of a meeting I will have on Wednesday with the potential Controller. In particular if and how this processing operation could be introduced in a mandatory legal basis for the presence control.

Best regards,

[redacted]

-----Original Message-----
From: [redacted]
Sent: 18 June 2018 10:10
To: [redacted]
Cc: Data Protection EP <Data-Protection@europarl.europa.eu>; HAROU Delphine <delphine.harou@edps.europa.eu>
Subject: RE: Nouveau dossier qui nécessite une discussion

Indeed dear [redacted], just to confirm that i am fully available on this matter.

Kind regards,
[redacted]

Legal Officer
Supervision and Enforcement Unit
European Data Protection Supervisor (EDPS)
[redacted]
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels

-----Original Message-----
From: HAROU Delphine
Sent: 18 June 2018 10:07
To: [redacted]
Cc: Data Protection EP <Data-Protection@europarl.europa.eu>; [redacted]
Subject: RE: Nouveau dossier qui nécessite une discussion

Hello [redacted],
[redacted] est disponible ce matin pour te répondre.
Belle journée à toi!
Delphine

-----Original Message-----
From: [redacted]
Sent: 15 June 2018 10:59
To: HAROU Delphine <delphine.harou@edps.europa.eu>
Cc: Data Protection EP <Data-Protection@europarl.europa.eu>
Subject: Nouveau dossier qui nécessite une discussion

Bonjour Delphine
Puis-je t'appeler lundi à propos d'un nouveau dossier "biométrie " qui vient de tomber sur mon bureau?
Quand serais-tu disponible après 10,30?
Merci et bonne fin semaine
[redacted]

Sent from my iPhone

EUROPEAN DATA PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Mr Joseph MIFSUD
Data Protection Officer
European Banking Authority (EBA)
Tower 42 (level 18)
25 Old Broad Street
London EC2N 1HQ
United Kingdom

Brussels, 13 October 2014
GB/MG/mjs/D(2014) 2032 **C 2014-0496**
Please use edps@edps.europa.eu for all correspondence

Subject: Prior checking notification concerning "Processing of leave and flexitime"

Dear Mr Mifsud,

On 30 April 2014, the European Data Protection Supervisor (EDPS) received from the European Banking Authority (EBA) the notification for prior checking concerning "Processing of leave and flexitime" (case 2014-0496).

The notification, accompanied by a "Specific Privacy Notice - Leave and Flexitime", contains the declaration that processing of personal data in the context of leave and flexitime by EBA is conducted in compliance with the EDPS guidelines concerning the processing of personal data in the area of leave and flexitime[1].

The organizational part of EBA entrusted with the processing of personal data is the "Operations Department/Human Resources staff in charge of administration of flexitime"; the concerned data subjects are temporary agents, contractual agents, seconded national experts working at EBA; and the purpose of the processing is "to monitor and measure the presence/absence of staff more effectively".

[1] Guidelines concerning the processing of personal data in the area of leave and flexitime adopted on 20 December 2012 (EDPS 2012-0158), available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/12-12-20_Guidelines_Leave_Flexitime_EN.pdf

Legal aspects

1. Prior checking

EBA states that the need for the prior checking notification under Article 27 of Regulation (EC) No 45/2001[2] (the Regulation) in this case is triggered by the intended use of a specific system (referred to at section 2 of this opinion) for the monitoring of the leave and absence of the staff (clock in/clock out). If such monitoring system had not been envisaged, "EBA flexitime system would in principle not be subject to prior checking" due to the fact that it does not explicitly include the evaluation of staff (conduct, efficiency) and that the data processed shall not be used in the staff appraisal procedure.

The EDPS recalls that the use of a certain technology as such is not, in principle, a reason to subject processing operations to prior checking pursuant to Article 27 of the Regulation. The EDPS does not prior check a data processing technology (a tool) as such but procedures implementing specified related purposes.
Hence, the EDPS concludes that the processing operations do not fall under the cases specifically laid down under the Regulation and therefore the data processing in question is **not subject to prior-checking**.

Without prejudice to the above considerations, the EDPS makes in this opinion a first assessment of compliance with the Regulation of the notified processing operations.

2. **Processing of personal data**: the Flexitime monitoring system (FMS)

As indicated in the notification, the Flexitime monitoring system (FMS) consists of "*a technology similar to fingerprints reader for the purpose of measurement of flexitime (clock-in, clock-out). The technology shall ensure that the fingerprints of the data subjects are neither read nor stored (...)". (...) the reader technology measures the change in electrical conductivity at a number of places across the reader surface and translates these readings into a unique 125 digit number. It is this unique number alone that is stored in the database for use when the data subject places his/her finger on the reader. (...) it shall not be possible to 'reverse engineer' the number into any form of finger pattern or fingerprint.*"

As first basic - and general - remark in view of the possible impact on data protection, the EDPS points out to the special sensitivity of (in this case, EBA staff members') biometric data[3].

---

[2] Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, published on the Official Journal of the European Union, 12.01.2001, L 8/1, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF

[3] Biometric data are peculiar in nature, being univocally linked to the individual, whose body is made 'readable'. See, in this regard, the Opinion of the WP29 of 27.04.2012, WP193 on developments in biometric technologies, available at:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

3. Lawfulness of processing

The lawfulness of the processing as regards the FMS must be considered in the light of Article 5(a) of the Regulation which reads: "personal data may be processed only if 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 or in the legitimate exercise of official authority vested in the Community institutions or body or in a third party to whom the data are disclosed". In this regard, Recital 27 of the Regulation also states that "Processing 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".

Based on its practice on supervision (where biometric-based systems have been accepted only in a limited number of cases, referring to the scenario – different than the one for which you consulted us – of access control for *security* purpose), the EDPS warns that the use of fingerprints-based systems for the monitoring of working time of staff members is **not** considered as **necessary**, and therefore, **not legitimate** pursuant to the aforesaid Article 5.

The requirement of the processing of personal data being necessary in relation to the purpose[4] obliges the controller to **assess whether the purpose of the processing could be achieved with less intrusive means**.
Indeed, **instead of opting** for a system using biometric data, other systems should have been considered by EBA in this context, such as: signing in, using attendance sheets, or using clocking in systems via magnetic badges.

4. Data quality

Article 4(1)(c) of the Regulation states that personal data must be "adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed."
The required data and their processing must be **proportionate** in the light of the purpose of the system (in this case, registering working time presence).

Since the requirement of the necessity of the processing of personal data for the aforesaid purpose is not fulfilled, the requirement of proportionality - laid down under the Article 4 of the Regulation - is also not met in this case.

[4] See, in this regard, on the use of biometric data, the Opinion of the WP29 of 27.04.2012, WP193: "*In analysing the proportionality of a proposed biometric system a prior consideration is whether the system is **necessary** to meet the identified need, i.e. is essential for satisfying that need rather than being the most convenient or cost effective. A second factor to take into consideration is whether the system is likely to be effective in meeting that need by having regard to the specific characteristics of the biometric technology planned to be used. A third aspect to weigh is whether the resulting loss of privacy is proportional to any anticipated benefit. If the benefit is relatively minor, such as an increase in convenience or a slight cost saving, then the loss of privacy is not appropriate. The fourth aspect in assessing the adequacy of a biometric system is to consider whether a less privacy intrusive means could achieve the desired end.*"

Conclusion

In the light of the above, the EDPS considers that the use of a biometric-based system for working time control (in this case, FMS) would **not** be compliant with the Regulation.

Yours sincerely,

Giovanni BUTTARELLI

p.o. G. Buttarelli

Cc: Mr Adam FARKAS, Executive Director, EBA

Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Anti - Fraud Office on CBIS Identity and Access Management System.

Brussels, 30 June 2008 (Case 2008-223)

1. Proceedings

On 11 April 2008, the European Data Protection Supervisor ("*EDPS*") received from the Data Protection Officer ("*DPO*") of the European Anti-Fraud Office ("*OLAF*") a notification for prior checking ("*the Notification*") regarding the data processing operations relating to the OLAF Identity and Access Management System operating on the Core Business Information Systems ("*CBIS*") infrastructure. .

The following documents were attached to the notification:
- Foundations for using Biometrics in OLAF's specific security systems;
- Match-on-Card Technology;
- Draft Privacy Statement for OLAF Identity and Access Management System.

On 24 April, the EDPS received additional information from the DPO regarding a pilot project envisaged by OLAF in the context of the processing operation. The EDPS requested additional information regarding the pilot project on 30 April and suspended the procedure. On 5 May, a meeting was held between the EDPS staff and OLAF to discuss the issues raised. The suspension of the procedure was lifted on 7 May, when additional information was provided to the EDPS regarding the pilot project. On 4 June 2008, a letter was sent from the EDPS analysing the acceptable conditions for the pilot project. On 5 June 2008, OLAF decided to withdraw the pilot project.

On 13 June, the EDPS sent the draft Opinion to the DPO of OLAF for comments which were received on 23 June 2008.

2. Examination of the matter

2.1. The facts

Scope of the notification

The Identity and Access Management System ("*IAMS*") is part of the security infrastructure that protects OLAF's core IT systems which in turn support OLAF investigations and all other activities to protect the financial interests of the European Union. The notification of OLAF

Identity and Access Management System is linked to the prior-check opinion that the EDPS adopted in relation to the OLAF's physical access control system[1].

The current prior check Opinion relates to processing of personal information carried out by OLAF, in particular the Information Services Division to ensure that only authorised persons have access to OLAF's core IT systems and to allow investigation of security incidents.

Processing

The OLAF IAMS is a directory service for IT systems and applications in the OLAF Secure IT environment, called Core Business Information Systems (*CBIS*). The IAMS will provide authentication and access control services in the CBIS environment. Logged access control events generated in the CBIS environment are kept in the CBIS Security Information and Events Management System (SIEMS).

According to the notification, OLAF considers that the implementation of this system is necessary to handle classified information.

The OLAF Information Security Policy ("*ISP*"), which has been developed in order to implement these security requirements within OLAF, requires a strong implementation of the Need-To-Know principle. This implies unequivocal identification, for instance strong authentication, of any user of OLAF's operations data processing systems.

OLAF annexed to the notification a note for the file on the "*Foundations for using Biometrics in OLAF's specific security systems*". This document explains why OLAF adopted biometrics technology to authenticate users of its specific security systems, from the perspective of Data Protection. The Commission's Information Systems SECurity POLicy ("*SECPOL*") defines three authentication factors: Authentication by Knowledge, by Ownership and by Characteristic.

OLAF decided to implement a two-factor authentication scheme based on "Ownership" and "Characteristic" for its two OLAF access control systems (physical and IT). According to the document provided to the EDPS, OLAF adopted fingerprints as the "Characteristic" authentication factor because OLAF concluded that it constitutes the best available compromise in terms of user-friendliness, reliability and cost. Other systems as hand-geometry, iris and retina characteristics were deemed more intrusive and/or more expensive. As "Ownership", OLAF uses a smartcard. Biometric data of users are stored only on the smartcard and it cannot be used for any other purpose.

Authentication in CBIS is based on digital certificates and fingerprints. Certificates are stored on the personal OLAF badges (smartcards) of users and protected by a biometric Match-on-card authentication scheme. Each user will have three fingerprint templates stored on his/her OLAF badge, which is a contact interface used by the CBIS IT authentication system.

Enrolment

The enrolment of a user consists of two independent processes:
a) The card's digital certificate will be registered in the access control system and linked to a person in the database;

[1] Opinion of 7 April 2008 on a notification for prior checking on identity and access control system (Case 2007-635) available on EDPS website.

b) The person's fingerprints from three fingers will be scanned by the system and a digital template representing the fingerprints will be calculated by the system and stored in the card only, not in a database. OLAF does not plan on using the card for any other purpose than Physical and IT access control.

Therefore, similar enrolment procedures are used for collecting the fingerprints which are used in both the physical and IT access controls. However, the templates are stored in two different chips.

Technical specificities

The technology used is based on the Precise 250 MC technology, whose specificities were sent by OLAF to the EDPS. It is a combined fingerprint and smart card reader system. The system stores and matches the fingerprint information in the secure environment of the card itself, and thereby eliminates the need for processing sensitive information in PCs and databases (Match-on-Card system).

The cards contain a digital certificate and three fingerprint templates for match on card biometric authentication. The reason for having three fingerprint templates is to reduce the risk of rejection.

The biometric template is the data that represents an enrolled fingerprint. It consists of two parts; the biometric header, which contains data about type and version of the biometric algorithm used, and the reference data, which contains the actual fingerprint characteristics. The reference data are computed and stored on the card at user enrolment time. The biometric algorithm works only one-way, the scanned fingerprints can not be reconstructed from the reference data.

The biometric reader scans a person's fingerprint and sends it to the contact chip which matches it with the stored fingerprint. If there is a positive match, the contact chip communicates the corresponding digital certificate to the logical access control system. Access will be granted or denied on the basis of authorisations programmed in the system for that badge.

According to the information provided, the EDPS sees that the False Rejection Rate ("*FRR*") which is used in all the contact chips is not precisely set but is "*estimated at 1:100*".

Moreover, ten tries per enrolled finger are possible before the system blocks the card.

The central database server is the administrative interface with the system. It stores information about the users and their access rights. It also stores any access attempts, granted or denied.

Legal basis
The legal basis of the processing is:

- Article 297 of the EC Treaty; Article 17 of the Staff Regulations;
- Regulation 1073/99 - Recitals 4, 17, 18; Articles 8, 11(1), 12(3);
- Commission Decision 1999/352: Recitals 4, 5; Article 3;
- Commission Decision 2001/844/EC, ECSC, Euratom (security provisions)
- Commission Decision 2006/3602/EC concerning security of information systems;
- Commission's IT security policy (PolSec);

Controller
The primary responsibility for the data processing lies within OLAF, in particular within the Information Services unit which provides all IT systems.

Data subjects
According to the notification, the following individuals are data subjects: Staff members working in the OLAF premises with the need to access the CBIS secure IT environment.

Categories of data concerned
The following categories of personal data are concerned:

- Personal identification data: name
- Organisational identification data: staff number, directorate, unit, sector
- Smartcard number
- Vetting information
- Fingerprint templates
- Application access rights: CBIS
- Physical access profile (family)
- Digital certificate

More specifically, the following data are logged by the Access Control System each time a badge is presented to a card reader: date; time; name; access granted or denied; access group name; card reader number and description.

Recipients of data
According to the notification, the CBIS recipients are OLAF staff responsible for CBIS access control. More precisely, the draft privacy statement sent to the EDPS states: "*OLAF HR and Security staff have access to information in the IAMS. OLAF IT and application support staff have access to the parts of the information that they need in order to manage the respective services that they provide to you*". There are no recipients outside of OLAF.

Automated/Manual processing

Automated: Users' identities and relevant access control information are provided to the IAMS from the Commission's Human Resources Management Systems' data warehouse ("*COMREF*"). The necessary data is automatically exported every night from COMREF and imported into the CBIS IAMS.

The IAMS controls access to the CBIS applications. Security events generated by CBIS systems are forwarded to the SIEMS. The SIEMS logs this information in order to allow control of security incidents.

Manual: The OLAF Human Resources ("*HR*") Unit can initiate a workflow that changes staff access rights in the CBIS environment. The OLAF units involved in managing CBIS systems and applications will approve or reject any change before it is executed.

Information given to data subjects
The notification states that a privacy statement will be available on the OLAF intranet.

The general privacy statement contains the following elements: explanation of the OLAF Access Control System; the personal information collected, for what purpose and through

which technical means; the recipients of the information and to whom it is disclosed; the protection and safeguards of the information; the retention period; the right of data subjects (access, modification, deletion) and finally the right to have recourse to the EDPS. The DPO included a draft of the privacy statement with the notification.

Rights of data subjects

The rights of the data subject are explained in the privacy statement in the following terms: "*You have the right to access the personal data we hold regarding you and to correct and complete them. Any request for access, rectification, blocking and/or erasing your personal data should be directed to Mr* [...], *Head of Unit D.8* [e-mail]. *You may also contact him in case of any difficulties, or for any question relating to the processing of your personal data. Exemptions under Article 20 (1)(a) and (b) of Regulation 45/2001 may apply*".

Moreover, the time limit to block data on justified legitimate request from the data subjects is established as 1 month.

Retention period

According to the notification and to the privacy statement, personal data will be deleted from the IAMS system when a person leaves OLAF, unless the person is a user of the Case Management System ("*CMS*"), in the case of which retention periods will be 20 years. Persons having had access to CMS will be disabled in the IAMS and all personal information, except the name and organisational entity of the user, will be deleted. Moreover, the smartcard will be erased and reused by another user or destroyed.

Logged access control events generated in the CBIS environment are kept for 1 year in the CBIS Security Information and Events Management System, which is part of the IAMS infrastructure.

As for the logical access control system, the specified retention period for logged access control is necessary because not all security incidents are discovered immediately. OLAF believes that a one year total retention period is reasonable in the case of OLAF, given the sensitive nature of its operational business.

Storage

The data is saved on a database on hard-disk and backup media. The storage of fingerprint templates is made on OLAF personal identification cards only.

Security measures

The notification contains a section on security measures. However, the information provided does not specifically relate to the IAMS alone. Indeed, the IAMS is protected by the same security standards applied to OLAF's Core Business Information Systems (CBIS). These have been analysed by the EDPS horizontally.

As to the security aspects, the Commission's IT Security policy and procedures apply to the OLAF IT infrastructure. Commission Decision 3602 of 17/08/2006 defines IT security measures in force. Its Annex I defines the security requirements of EC Information Systems. Annex II defines responsibilities of the various actors. Annex III defines the rules applicable to users.

For the provision of the other information systems under its responsibility, OLAF currently relies on the EC corporate IT network infrastructure (Telecom Centre + SNET) and on EC corporate Users provisioning/authentication security services (e.g. the NET1 MS Active Directory, LDAP and ECAS) provided centrally by DIGIT for all Commission DG's and services.

Furthermore, the privacy statement contains a chapter on security aspects which reads as follows: "*In order to protect your personal data, a number of technical and organisational measures have been put in place (...)*

(...)

2.2. Legal aspects

2.2.1. Prior checking

This prior check Opinion relates to processing of personal information carried out by OLAF, in particular the Information Services unit, to ensure that only authorised persons have access to OLAF's core IT systems and to allow investigation of security incidents. As already explained above, the notification of the CBIS access control at OLAF is linked to the prior-check opinion that the EDPS adopted in relation to OLAF's physical access control system[2].

Regulation (EC) No 45/2001[3] 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*" and to the processing "*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 described below, all elements that trigger the application of the Regulation are present:

First, *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001 are collected and further processed. Second, the personal data collected undergo *"automatic processing"* operations, as defined under Article 2(b) of the Regulation (EC) No 45/2001, as well as manual data processing operations. Indeed, the personal data such as personal identification data and fingerprints are collected and undergo 'automatic processing', for example when the information service takes the templates of fingerprints. Moreover, manual processing can be implemented by OLAF's Human Resources unit or the Information Services Unit managing the CBIS system. Finally, the processing is carried out by a *Community body*, in this case by the European Anti-Fraud Office, in the framework of Community law (Article 3(1) of the Regulation (EC) No 45/2001). Therefore, all the elements that trigger the application of the Regulation are present in this processing operation.

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 subjects by virtue of their nature, their scope or their purposes"*. The EDPS considers that the presence of some biometric data other than photographs alone, such as the case in point where biometric fingerprints are collected, presents specific risks to the rights and freedoms of data subjects. This view is mainly based on the nature of biometric data which are highly sensitive, due to some inherent characteristics of this type of data. For example, biometric

[2] See footnote 1.

[3] Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ("Regulation (EC) No 45/2001").

data change 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 addition to the highly sensitive nature of the data, the EDPS also notes that possibilities of inter-linkage and the state of play of technical tools may produce unexpected and/or undesirable results for data subjects. These risks justify the need for the data processing to be prior checked by the EDPS in order to verify that stringent safeguards have been implemented.

Since prior checking aims at addressing situations that are likely to present certain risks, the opinion of the EDPS should be given prior to the start of the processing operation. The current opinion constitutes a **true prior check**. Therefore, such processing should not be implemented until the recommendations of this opinion are taken into account and the EDPS is informed of the measures of implementation (see Article 27(4) third paragraph), unless specific timing is stated (see Conclusion)

The notification was received on 11 April 2008. 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 8 days to obtain additional information plus 10 days to allow comments on the draft Opinion. The Opinion must therefore be adopted no later than 30 June 2008.

2.2.2. Lawfulness of the processing

Personal data may only be processed if grounds can be found in Article 5 of Regulation (EC) No 45/2001.

Of the various grounds listed under Article 5 of Regulation (EC) No 45/2001, the processing operation notified for prior checking falls under Article 5 a), pursuant to which data may be processed if the processing is "*necessary for 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 or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed"*

In order to determine whether the processing operations comply with Article 5 a) of Regulation (EC) No 45/2001, three elements must be taken into account: First, whether either the Treaty or other legal instruments foresee the data processing operations carried out; second, whether the processing operations are performed in the public interests; and, third, whether the processing operations are indeed necessary for the performance of that task (necessity test). Obviously, the three requirements are closely related.

* The **legal basis** for the processing is to be found in:

- Article 297 of the EC Treaty; Article 17 of the Staff Regulations;
- Regulation 1073/99 - Recitals 4, 17, 18; Articles 8, 11(1), 12(3);
- Commission Decision 1999/352: Recitals 4, 5; Article 3;
- Commission Decision 2001/844/EC, ECSC, Euratom (security provisions)
- Commission Decision 2006/3602/EC concerning security of information systems;
- Commission's IT security policy (PolSec);

* Processing operations are carried out **in the legitimate exercise of official authority.** The EDPS notes that the Commission carries out the processing activities in the legitimate exercise of its official authority. Indeed, the processing operations take place in the

framework of a mission carried out in the public interest on the basis of the Staff Regulations of the officials of the European Communities and the conditions of employment of other servants of the European Communities, as well as the OLAF Information Security Policy. The admissibility of the treatment is thus respected.

* As to the necessity of the processing **(necessity test),** according to Article 5 a) of Regulation (EC) No 45/2001, the data processing must be "*necessary for performance of a task*" as referred to above. In this respect, recital 27 of Regulation (EC) No 45/2001 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*".

OLAF's mission is the protection of the financial and other interests of the Community against fraud and irregular conduct liable to result in administrative or criminal proceedings. Moreover, OLAF shall exercise the powers of the Commission in order to step up the fight against fraud, corruption and any other illegal activities detrimental to the Communities' financial interests[4].

Taking into account the relevance of these interests and in order to prevent the unauthorized access and disclosure of this sensitive information, OLAF could indeed find it necessary to adopt special security measures, including the setting up of stringent access control systems for its IT systems and to allow investigation of security incidents at OLAF. Therefore, in the EDPS' view, the implementation of strong access control systems which entail the processing of personal data can in this case reasonably be considered as a necessary internal control measure towards the safeguard of financial information and other interests of the Community.

2.2.3. Processing of special categories of data

The notified data processing does not relate to data falling under the categories of data referred to in Article 10.1 of Regulation (EC) No 45/2001.

2.2.4. 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 analysing whether the processing at issue here, which involves mainly the processing of biometric data, is in line with this principle, the EDPS notes the following:

As stated in the notification, each member of OLAF staff with the need to access the CBIS secure IT environment is considered to be a data subject.

Further, the notification describes that the system is a directory service for IT systems and applications on the OLAF Secure IT environment. Logged access control events generated in the CBIS environment are kept in the CBIS Security Information and Events Management System, which is part of the IAMS infrastructure.

Authentication in CBIS is based on digital certificates and fingerprints. Certificates are stored on users' personal OLAF badges (smartcards) and protected by a biometric match on card

[4] OLAF Manual, p. 13.

authentication scheme. Each user will have three fingerprint templates stored on his/her OLAF badge.

As a consequence, each member of OLAF staff with the need to access the CBIS secure IT environment must carry an OLAF badge in order to be authorised to access the OLAF IT environment. The EDPS understands that only those persons who need access to the CBIS secure IT environment need to enrol their fingerprints in the contact chip.

Moreover, in the notification, OLAF provided the EDPS with documents supporting the reasons for using Biometrics in OLAF's specific security systems. The OLAF Information Security Policy, which has been developed in order to implement the security requirements within OLAF, requires a strong implementation of the Need-To-Know principle. This implies unequivocal identification, for instance strong authentication, of any user of OLAF's operational data processing systems. In the context of OLAF's access control, the EDPS interprets this Need-To-Know principle as requesting that only the people who need special access should be enrolled in the system and therefore be fingerprinted.

The type of data collected, mainly the fingerprint templates of three fingers and related identification information, corresponds to the data required to operate an access control system based on biometrics. From this point of view, the EDPS considers that the data collected are adequate and relevant for the purposes of the processing.

Fairness and lawfulness. Article 4(1)(a) of the Regulation requires that data be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section 2.2.2). The issue of fairness is closely related to what information is provided to data subjects, which is further addressed in Section 2.2.9.

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 personal data at stake include mainly biometric data, used for access control purposes to IT systems. Some key features of biometric systems have a direct impact on the level of accuracy of the data generated either in the enrolment or identification phases inherent to this type of system. Depending on whether the biometric system is set up in a way that integrates these key elements, the accuracy of the data will be (or not) at stake. The EDPS analysed in his Opinion relating to OLAF physical access control the rules to be followed when implementing biometric systems. Next we describe these key elements and analyse the extent to which they have been taken into account in the biometric IT access control system concerned.

- First, any enrolment phase must foresee alternative ways to identify individuals who are not eligible, even temporarily, for enrolment, for example because of damaged fingerprints. This is usually referred to as ***"fall back procedures"***[5]. According to the additional information provided and the analysis of the physical access control system, OLAF has not foreseen any Failure to Enrol Rate ("*FER*"), as it anticipates that all staff will be able to enrol.

[5] For a description of the data protection principles applicable in relation to fall back procedures, see Opinion of 13 October 2006 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 C 313, 20.12.2006, p. 36.

After analysis, the EDPS concludes that although OLAF anticipates that all staff will be able to enrol, it has implemented a fallback procedure in the sense that three fingerprint templates, and not only one, are taken during the enrolment phase. During the biometrics authentication process, the user will place one of the three fingers that he/she had chosen at enrolment time.

Although this solution diminishes the risk of failure to enrol, it is still possible that some people may not be able to enrol through the fingerprint system. In such a case, it would be discriminatory for the person concerned: let alone, if the failure to enrol would prevent the person to fulfil his/her contractual obligations. Therefore, the EDPS suggests that OLAF should develop a workable alternative solution if and when a case of permanent impossibility to enrol occurs. This solution will have to take into account the level of security risk of the CBIS and should also preserve the rights of the data subject(s) concerned.

- Second, similar types of measures must be foreseen for those individuals who are properly enrolled but who are wrongly identified (usually referred to as "***false rejection***"). If these measures are not embedded in the architecture of the system, the accuracy of the information produced by the system may be compromised. In particular, in the case of false rejection, the system will produce a record that a given individual without proper access rights intended to access an IT environment system, when in fact the individual did have such rights. At the same time, because the individual will be misidentified, he/she will be denied access to the secure CBIS IT environment of OLAF.

  Regarding OLAF's access control system, according to the information provided to the EDPS, the False Rejection Rate ("*FRR*") which is used is "*estimated at 1:100*", and determined by the level of security expected within OLAF IAMS. The EDPS has some comments regarding this aspect:

  1. The EDPS is surprised to see that the FRR is not precisely defined but is rather "estimated". This rate is usually based on the security policy of the operator who will select a threshold under which fingerprint will always be rejected in order to mitigate the risk that an impostor will have access to the data.

  2. The EDPS is also surprised to see that OLAF decided to implement a FRR rate which is identical to the one which is used for the physical access control to OLAF building. Indeed, in the case of CBIS, access is directly granted to data in IT systems and a higher level of security could be expected. Therefore, the EDPS would like OLAF to select a precise FRR for the CBIS system which will reflect the security policy it has adopted.

  3. Moreover, in the case of a false rejection, the EDPS suggests that OLAF develop a procedure which should address the problem in a way that does not put too much burden upon individuals. In other words, the alternative procedure should provide sufficiently simple solutions to the problem of misidentification and rejection. In this respect, the EDPS would like that OLAF establish a periodical renewal of enrolment in order to maintain a high level of data quality. The establishment of a renewal period is justified, for instance, because biometrics, especially fingerprints may evolve with the life of a data subject. It is also justified by the possible change in the skin condition of relevant finger of the user over the time, as well as by the quality of the

enrolled fingerprint template. This renewal period could be defined and implemented after one year of operation of the new system, on the basis of the experience faced by OLAF with the system. This also underlines the importance for OLAF to establish a precise FRR.

- Finally, OLAF logical access control system is based on fingerprint templates stored in cards and which are combined with the use of readers. Contrary to the OLAF physical access control, the OLAF logical access control system does implement a 100% "Match-on-Card" authentication scheme. The EDPS welcomes this system, which avoids further unlawful uses and phishing expeditions which often appear with the use of databases[6].

2.2.5. Conservation of data/ Data retention

Article 4(1)(e) of Regulation (EC) No 45/2001 sets forth the principle that "*personal data must be kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the data were collected or for which they were further processed". "The Community institution or body shall lay down that personal data which are to be stored for longer periods for ... statistical use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subject encrypted."*

According to the general notification, personal data will be deleted from the IAMS system when a person leaves OLAF, unless the person is a user of the Case Management System (CMS) in the case of which the retention period of 20 years applies. Persons having had access to CMS will be disabled in the IAMS and all personal information, except the name and organisational entity of the user, will be deleted. The smartcard will be erased and reused by another user or destroyed.

Moreover, logged access control information will be kept for one year. The data are needed for investigating security incidents. As justification, OLAF mentions that the specified retention period is necessary because not all security incidents are discovered immediately. For example, some security investigations were triggered two to three years after the leak of a sensitive OLAF operational document. Therefore, OLAF believes that a one year total retention period is reasonable in the case of OLAF, given the sensitive nature of its operational business.

The EDPS considers that timing is a key element in the discovery of security incidents. Indeed, the more sensitive a system is, the earlier the detection of security incidents has to take place. The EDPS understands that it may be necessary to keep an audit trail of the registering data for a period of time which allows reconstructing events during security related incidents and that in the case of OLAF, it may not be practical to have a very short period. The EDPS assumes that OLAF has in place or, if not, should develop a process of identifying and responding to incidents so that they are detected and reported as soon as possible after they have occurred. Presumably OLAF aims at discovering incidents immediately after they take place and in any case no later than several months thereafter. Based on the foregoing, the EDPS feels that the period of one year is long and invites OLAF to reconsider the setting of its conservation period by reassessing the need to shorten this time by using the statistics of incidents. Therefore, the storage period should be determined by the time it usually takes for OLAF to discover a security incident from the moment that it took

[6] See Opinion on a notification for prior checking received from the Data Protection Officer of the European Central Bank related to the extension of a pre-existing access control system by an iris scan technology for high secure business areas, 14 February 2008 (2007-501) available on the EDPS website.

place. The EDPS understands that OLAF does not have such statistics on incidents but that it will be able to re-evaluate the initial retention period after one year of operation of its new system. Therefore, the EDPS agrees that OLAF proposes a new retention period on the basis of statistics available by then.

As regards the time limit to block/erase data on justified legitimate request from the data subjects, it is set at one month. The EDPS considers that this retention period complies with the requirements set out in Article 4(1)(e) of the Regulation.

The EDPS understands from the notification that no statistics on personal data are allowed after the retention period. Nevertheless, the EDPS would emphasise that where such data are used beyond the retention period, they must be made anonymous (Article 4(1)(e) of the Regulation).

2.2.6. Transfer of data

According to the notification and the privacy statement, OLAF HR and Security staff members have access to information in the IAMS.

The EDPS recalls that Article 7 of Regulation (EC) No 45/2001 requires that personal data be transferred if it is "*necessary for the legitimate performance of tasks covered by the competence of the recipient"*. In order to comply with this provision, in sending personal data, OLAF must ensure that (i) the recipient has the appropriate competences and (ii) the transfer is necessary. The EDPS considers that this is the case for reporting security incidents in this instance. However, whether a given transfer meets such requirements will have to be assessed on a case-by-case basis. In addition to the above, pursuant to Article 7 of Regulation (EC) No 45/2001 a notice has to be given to the recipient in order to inform him/her that personal data can only be processed for the purposes for which they were transmitted.

2.2.7. Processing of personal number or unique identifier

Article 10(6) of the Regulation provides that "*the European Data Protection Supervisor shall determine the conditions under which a personal number or other identifier of general application may be processed by the Community institution or body"*. The present opinion will not establish the general conditions of such a use of a personal number, but consider the specific measures necessary in the context of an "Access Control" system.

The EDPS has already clarified, in a previous prior-checking opinion[7], the status of an embedded RFID chip number in a card. The identification number associated to the RFID chip is personal data covered by Regulation 45/2001. Indeed, this identification number when used to record a staff member's behaviour and linked to the personnel number (which means linked to the name of a person, as is the case here), makes this a processing of personal data, which requires compliance with the data protection principles.

The use of the personal number is necessary because the card ID is communicated to the access control system. For the case in hand, the use of the staff personnel number for the purpose of verifying the access right data in the system is reasonable considering that this number is used to identify the person in the system and thus helps ensure that the data are accurate.

[7] See Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission on "the implementation of flexitime - specific to DG INFSO", 19 October 2007 (2007-218).

2.2.8. 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 prior checking notification and the supplementary information submitted by the controller describe the possibility of access to and mention the possibility of rectification of personal data by a staff member.

According to the prior checking notification and the supplementary privacy statement submitted by the controller, the rights of access and rectification are recognized. The privacy statement which was submitted to the EDPS for review provides the name of the person responsible for the execution of these rights. The EDPS recalls that these rights apply not only to the information provided by the individual (identification information and fingerprint templates) but also to the information generated every time an individual accesses the CBIS secure IT system.

The EDPS notes that, according to the notification, Article 20 of Regulation 45/2001 is not to be applied, in principle, in the context of this data processing operation.

In conclusion, the EDPS considers that the conditions of Articles 13 and 14 of the Regulation are met.

2.2.9. Information to the data subject

Articles 11 and 12 of Regulation (EC) 45/2001 list information that must be provided to the data subjects. These articles list a series of compulsory items and another set of information.

The latter are applicable insofar as, taking into account the particular circumstances of the treatment in question, they are necessary in order to ensure a fair data processing with regard to the data subject. In this case, part of the data is collected directly from the data subject and another part from other people.

Data subjects are informed by a "*privacy statement for OLAF identity and access management system*". In order to show compliance with these articles, a draft of the privacy statement was provided to the EDPS.

The EDPS also reviewed the content of the information provided in the privacy statement to verify whether the content satisfies the requirements of Articles 11 and 12 of Regulation (EC) No 45/2001. The privacy statement contains information on the purposes of the processing and how the data are processed, the conditions for the exercise of the right of access and rectification, the time limits for storing the data and the possibility to have recourse to the EDPS. The EDPS considers that the privacy statement contains most of the information required under Articles 11 and 12 of the Regulation. However, he considers that some amendments would contribute to ensure full compliance with Articles 11 and 12, in particular:

- Mention whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply (for instance, the consequences of failure

to enrol). By analogy with a questionnaire, the staff should be informed of the practical consequences to enrol and of failure to do so;

- Indicate that, if necessary, the information may be transferred for the purposes of carrying out an administrative inquiry.

Besides, the privacy statement is supposed to be provided to individuals who undergo an enrolment phase in order to access CBIS IT system. In another prior-checking analysis[8], the EDPS acknowledged the procedure implemented at the ECB (i.e. "*the privacy statement will be provided* [o]*n paper and individuals will be asked to sign it stating that they have read and understood the statement*"). The EDPS considers that this is an appropriate method of providing the information and suggests that a copy of the privacy statement be given to individuals so that they can go back to the privacy statement in case, for example, they want to know how to exercise their rights or how the data processing takes place.

2.2.10. Security measures

According to Article 22 of the Regulation, the controller must implement the 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. These security measures must in particular prevent any unauthorized disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other forms of unlawful processing.

The EDPS notes that OLAF's specific IT infrastructure has been horizontally reviewed by the EDPS in a separate procedure. This prior checking Opinion is not the place to repeat that review.

(...)

3. Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 provided that the considerations in this Opinion are fully taken into account. In particular, OLAF should,

A) *before* implementing the intended processing operations:

- Ensure that only the persons who need access to the CBIS secure IT environment need to enrol their fingerprints in the contact chip;
- Define a precise FRR corresponding to the specific security level of CBIS;
- Amend the privacy statement as recommended in this Opinion and ensure that a copy of the privacy statement is given to individuals, or that it is made available to them in a way that allows them to consult it;

B) *after* the processing operations have started:

- When a case of permanent impossibility to enrol occurs, develop a workable alternative solution, which takes into account the impossibility of staff to be fingerprinted at the enrolment phase;

[8] See Opinion on the European Central Bank access control (2007-501).

- After one year of operation, consider periodical renewal of OLAF staff members' enrolment or develop alternative measures to deal with false rejections;
- Reconsider the setting of the conservation period of data after the first year of operation of the new system;
- Ensure that, if in the future data transfers take place, notices are sent to Community institutions receiving data processed in the context of the access control system, informing them that the personal data can only be processed for the purposes for which they were transmitted;

Done at Brussels, 30 June 2008

(signed)

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor