To be filled out in the EDPS' office

REGISTER NUMBER: 357

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 10/04/2008

Case number: 2008-223

Institution: OLAF

Legal basis: article 27-5 of the regulation CE 45/2001(1)

(1) OJ L 8, 12.01.2001

INFORMATION TO BE GIVEN(2)

(2) Please attach all necessary backup documents

1/ Name and adress of the controller

2) Name and First Name of the Controller:SONNBERGER Harald

3) Title:Head of Unit

4) Directorate, Unit or Service to which the Controller is attached:D.08

5) Directorate General to which the Controller is attached:OLAF

2/ Organisational parts of the institution or body entrusted with the processing of personal data

26) External Company or Directorate General to which the Processor is attached:
25) External Company or Directorate, Unit or Service to which the Processor is attached:

3/ Name of the processing

CBIS Identity & Access Management System

4/ Purpose or purposes of the processing

To ensure that only authorised persons have access to OLAF's core IT systems and to allow investigation of security incidents

5/ Description of the category or categories of data subjects

14) Data Subject(s) concerned:

Staff members working in the OLAF premises with the need to access the CBIS secure IT environment.

16) Category(ies) of Data Subjects:

All categories of OLAF staff working within the OLAF secure premises with the need to access the CBIS secure IT environment.

6/ Description of the data or categories of data (including, if applicable, special categories of data (article 10) and/or origin of data)*(including, if applicable, special categories of data (article 10) and/or origin of data)*

17) Data field(s) of Data Subjects:

Attention: Please indicate and describe in the answer to this question also data fields which fall under article 10

Personal identification data: name
Organisational identification data: staff number, directorate, unit, sector
Smartcard number
Vetting information
Finger prints
Application access rights: CBIS
Physical access profile (family)

18) Category(ies) of data fields of Data Subjects:

Attention: Please indicate and describe in the answer to this question also categories of data fields which fall under article 10

Personal identification data: name
Organisational identification data: staff number, directorate, unit, sector
Smartcard number
Vetting information
Finger prints
Application access rights: CBIS
Physical access profile (family)

7/ Information to be given to data subjects

15a) Which kind of communication(s) have you foreseen to inform the Data Subjects as described in articles 11 - 12 under 'Information to be given to the Data Subject'

The attached privacy statement will be available on the OLAF intranet.

8/ Procedures to grant rights of data subjects (rights of access, to rectify, to block, to erase, to object)*(rights of access, to rectify, to block, to erase, to object)*

15b) Which procedure(s) did you put in place to enable Data Subjects to exert their rights: access, verify, correct, etc., their Personal Data as described in articles 13 - 19 under 'Rights of the Data Subject' :

See attached privacy statement

9/ Automated / Manual processing operation

7) Description of Processing:

Attention: Please describe in the answer to this question if you process personal data falling under article 27 "Prior-Checking (by the EDPS - European Data Protection Supervisor)"

The OLAF Identity & Access Management System (IAMS) is a directory service for IT systems and applications on 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, 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 authentication scheme. Each user will have three fingerprint templates stored on his/her OLAF badge.
Annex 1 provides an explanation of the reasons that OLAF opted for biometrics authentication on CBIS.
Annex 2 provides a description of the match-on-card biometrics authentication technology used by OLAF.

8) Automated Processing operation(s):

Users' identities and relevant access control information are provided to the IAMS from the Commissions 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 Security Information Event Management system (SIEMS), which is part of the IAMS solution. The SIEMS logs this information in order to allow control of security incidents.

9) Manual Processing operation(s):

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.

10/ Storage media of data

Database on Hard-disk and backup media.
Fingerprint templates data are stored on the OLAF personal identification card only.

11/ Legal basis and lawfulness of the processing operation

11) Legal basis of Processing:

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);
OLAF Information Security Policy (Section 4.5 of the OLAF Manual).

12) Lawfulness of Processing:

Answering this question please also verify and indicate if your processing has to comply with articles 20 "Exemptions and restrictions" and 27 "Prior checking (by the EDPS)"

The Identity and Access Management System is part of the security infrastructure that protects OLAFs core IT systems which in turn support OLAF investigations and all other activities to protect the financial interests of the European Union. Thus, the processing is lawful because it is necessary for the performance of a task carried out in the public interest on the basis of the Treaties or other legal instruments, in accordance with Article 5(a).
The exemptions and restrictions of Article 20 do not apply.
This processing operation is subject to prior checking in accordance with Article 27(2)(a) of Regulation 45/2001.

12/ The recipients or categories of recipient to whom the data might be disclosed

20) Recipient(s) of the Processing:

OLAF staff responsible for CBIS access control; no recipients outside of OLAF.

21) Category(ies) of recipients:

OLAF staff responsible for CBIS access control; no recipients outside of OLAF.

13/ retention policy of (categories of) personal data

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 as notified under DPO-073 apply. 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.

13 a/ time limits for blocking and erasure of the different categories of data (on justified legitimate request from the data subject) (Please, specify the time limits for every category, if applicable)
(on justified legitimate request from the data subject)
(Please, specify the time limits for every category, if applicable)

22 b) Time limit to block/erase data on justified legitimate request from the data subjects

1 Month

14/ Historical, statistical or scientific purposes

If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification,

22 c) Historical, statistical or scientific purposes - If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification

15/ Proposed transfers of data to third countries or international organisations

27) Legal foundation of transfer:

Only transfers to third party countries not subject to Directive 95/46/EC (Article 9) should be considered for this question. Please treat transfers to other community institutions and bodies and to member states under question 20.

Not applicable.

28) Category(ies) of Personal Data or Personal Data to be transferred:

Not applicable.

16/ The processing operation presents specific risk which justifies prior checking (please describe):*(please describe)*):

7) Description of Processing:

Attention: Please describe in the answer to this question if you process personal data falling under article 27 "Prior-Checking (by the EDPS - European Data Protection Supervisor)"

The OLAF Identity & Access Management System (IAMS) is a directory service for IT systems and applications on 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, 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 authentication scheme. Each user will have three fingerprint templates stored on his/her OLAF badge.
Annex 1 provides an explanation of the reasons that OLAF opted for biometrics authentication on CBIS.
Annex 2 provides a description of the match-on-card biometrics authentication technology used by OLAF.

12) Lawfulness of Processing:

Answering this question please also verify and indicate if your processing has to comply with articles 20 "Exemptions and restrictions" and 27 "Prior checking (by the EDPS)"

The Identity and Access Management System is part of the security infrastructure that protects OLAFs core IT systems which in turn support OLAF investigations and all other activities to protect the financial interests of the European Union. Thus, the processing is lawful because it is necessary for the performance of a task carried out in the public interest on the basis of the Treaties or other legal instruments, in accordance with Article 5(a).
The exemptions and restrictions of Article 20 do not apply.
This processing operation is subject to prior checking in accordance with Article 27(2)(a) of Regulation 45/2001.

 Article 27.2.(a) Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

Yes, because of the presence of biometric fingerprints.

 Article 27.2.(b) Processing operations intended to evaluate personal aspects relating to the data subject,

No.

 Article 27.2.(c) Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,

No.

 Article 27.2.(d) Processing operations for the purpose of excluding individuals from a right, benefit or contract,

No.

 Other (general concept in Article 27.1)

No.

17/ Comments

1) Date of submission:

10) Comments if applicable:

36) Do you publish / distribute / give access to one or more printed and/or electronic directories?

Personal Data contained in printed and/or electronic directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.
If Yes, please explain what is applicable.

no

37) Complementary information to the different questions if applicable, including attachments to this notification which should not be public :

PLACE AND DATE:10/04/2008

DATA PROTECTION OFFICER: LAUDATI Laraine

INSTITUTION OR BODY:OLAF