(To be filled out in the EDPS' office)
REGISTER NUMBER:

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 07/02/2013

CASE NUMBER: 20130163

INSTITUTION: EUROPEAN PARLIAMENT

LEGAL BASIS: ARTICLE 27-5 OF THE REGULATION CE N° 45/2001([1])

INFORMATION TO BE GIVEN[2]

1/ NAME AND ADDRESS OF THE CONTROLLER

MATHIEU THOMANN
DIRECTOR, DIRECTORATE FOR SECURITY & RISK ASSESSMENT
EUROPEAN PARLIAMENT, ASP 01H356, RUE WIERTZ 60, B- 1047 BRUSSELS

2/ ORGANISATIONAL PARTS OF THE INSTITUTION OR BODY ENTRUSTED WITH THE PROCESSING OF PERSONAL DATA

DIRECTORATE FOR SECURITY & RISK ASSESSMENT - DG PRESIDENCY

3/ NAME OF THE PROCESSING

Risk Based Access Management to the European Parliament

4/ PURPOSE OR PURPOSES OF THE PROCESSING

A risk based access to the EP.
When the outcome of a risk analysis (established in accordance with Notifications 237 & 240) concerning a person shows that future access authorisation could pose a security risk to the Institution, access of that person to the EP may be restricted in order to protect the

[1] OJ L 8, 12.01.2001.

[2] **Please attach all necessary backup documents**

safety and security of the EP, its premises, and/or its users. If the risk is considered too high, the person may be placed in one of two categories, depending on the level of risk:

Category 1 - Access to the EP denied.
Category 2 - Access to the EP permitted, subject to notification by the Accreditation Unit (AU) to the Risk Management Unit (RMU) when access is requested. No authorisation by the RMU is required, the person has regular access. RMU decides whether the risk level for other events or assets changes based on the presence of the person in question.

For information, risk analyses are conducted on a case-by-case basis when competent staff members of the Directorate for Security and Risk Assessment have reasonable grounds to suspect a potential breach of security or any other security incidents or threats to the EP's premises and its users.
Besides helping to define the exact subject and limitations of the analysis, this ensures compliance with Article 4 of the Regulation 45/2001 by reducing the processing of personal data to only the relevant data necessary for the purpose for which they have been collected.
Personal data processed in the context of a risk analysis are possibly collected from:
- inviting party;
- the Accreditation Unit;
- the Internal Security Unit;
- the Press Unit (DG COMM);
- other EU institutions or Member States;
- third countries;
- open sources (internet and newspapers).

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

Persons for whom the outcome of a risk analysis (established in accordance with Notifications 237 & 240) shows that future access authorisation could pose a security risk to the Institution.

6 / DESCRIPTION OF THE DATA OR CATEGORIES OF DATA *(including, if applicable, special categories of data (Article 10) and/or origin of data)*

Digital File:
If available: First and Last Name, Date of Birth, ID number, Nationality, Address.
Date of decision to list the individual, competent authority, date of last update of the file, category (1 or 2)

Hard-copy File
The information contained in the digital file, plus the risk analysis, any relevant correspondence on the issue, and the request by the competent authority. (All irrelevant personal data is destroyed after the risk analysis is drawn-up).

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

- Where their contact details are available, individuals are informed in writing by the Directorate for Security and Risk Assessment of the decision to refuse them access to the EP when they are placed in Category 1

- People placed in Category 2 have normal access to the Parliament and therefore the general terms apply to them, as to all other visitors. For this purpose, a notice on data protection and individual rights is available for all visitors at all entrances as well as on the internet web-site of the EP.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS (Rights of access, to rectify, to block, to erase, to object)

- Individuals placed in Category 1 may appeal the decision to the Deputy Secretary General by registered mail within 10 working days of being notified.

- For individuals placed in Category 2, see under point 7.

9/ AUTOMATED / MANUAL PROCESSING OPERATION

Manual processing

10/ STORAGE MEDIA OF DATA

- The digital data is stored in the EP network in a specific directory and file for the Risk Management Unit (RMU) in the Directorate of Security and Risk Assessment (DS). Access to computer system is restricted to authorised staff of the DS.

- The RMU keeps the hard-copy files in a locked cabinet with highly restricted access

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

The Decision by the Bureau of the European Parliament of 18 March 2009.
The Decision by the Bureau of the European Parliament of 6 July 2011 on the Global Security Concept.

12/ THE RECIPIENTS OR CATEGORIES OF RECIPIENT TO WHOM THE DATA MIGHT BE DISCLOSED

In rare cases, information gathered in the framework of this processing operation may be disclosed to the security services of other European Institutions or EU Member States when relevant for national security or for the security of those institutions. In such cases disclosure is limited to the information relevant to the receiving party only, and subject to approval by the EP competent authority.
Thus, personal data are transferred in full compliance with Articles 7 and 8 of Regulation 45/2001 (and notably the necessity and competence principles). Recipients are reminded

orally or in writing that they cannot use the transferred data for any purpose other than the security purpose/investigation at stake.

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

Placement in one of the categories will be for a period of between one and three years, according to a case by case analysis. After this period restrictions are lifted, unless a new decision is provided. Once restrictions are lifted for a person, his or her personal data are completely deleted from the digital file.

Hard-copy files will be kept for 10 years after restrictions are lifted, as is the case for all types of investigations and risk analyses (see Notifications 237 & 240). This prolonged period of time is necessary to guarantee continuity and the availability of a complete dossier which is essential in case of further security or safety incidents after restrictions have been lifted. In addition, in Belgium a judicial file can be reopened within ten years, in which case certain information may be necessary.

13 A/ TIME LIMIT TO BLOCK/ERASE ON JUSTIFIED LEGITIMATE REQUEST FROM THE DATA SUBJECTS

(Please, specify the time limits for every category, if applicable)

See point 8 (reaction required within 10 working days)

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.

Not applicable

15/ PROPOSED TRANSFERS OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

See point 12. No transfers to third countries take place

16/ THE PROCESSING OPERATION PRESENTS SPECIFIC RISK WHICH JUSTIFIES PRIOR CHECKING *(Please describe):*

AS FORESEEN IN:

☐ Article 27.2.(a)

Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

☐ Article 27.2.(d)

Processing operations for the purpose of excluding individuals from a right, benefit or contract,

أ

17/ COMMENTS

PLACE AND DATE: XX FEBRUARY 2013

DATA PROTECTION OFFICER: SECONDO SABBIONI

INSTITUTION OR BODY: EUROPEAN PARLIAMEN