DATA PROTECTION SERVICE

NOTIFICATION

OF PERSONAL DATA PROCESSING

Art. 25 of Regulation (EC) 45/2001 of the European Parliament and the Council of 18 December 2000

EUROPEAN PARLIAMENT

(For the use of Data Protection Service)

Notification no.:

Date received: 12-02-2019

In accordance with Regulation (EC) 45/2001, individuals whose personal data are processed by the European Parliament in any context whatsoever are to be protected with regard to the processing of personal data.

1. IDENTIFICATION OF THE DATA CONTROLLER OR ANY SYSTEM

The data controller is the unit or other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data.

SURNAME [redacted] Given name [redacted] E-mail [redacted]

Function **Head of Unit**

Administrative Address: Building and room [redacted] Tel. [redacted] Place of work **Luxembourg**

Personal data filing system means any structured set of personal data accessible according to specific criteria

Name of filing system **Multifunctional devices for printing, copying and scanning with authentication process**

Instance(s) responsible for processing **Printing Unit**

Building and room [redacted] Place of work **Luxembourg**

2. PURPOSE AND LEGAL BASIS OF PROCESSING

Personal data must be processed only for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

2.1 Indicate the purpose of this processing of personal data (Please, described the procedure linked to this operation):

The multifunctional devices (MFDs) use personal data to provide more efficiency, more security, and modern new features. It gives the possibility to send jobs for printing (files to print) from PCs or mobile devices.

These devices require user authentication:
- The first time: necessity to register the EP badge (ID and password from the EP LDAP required),
- The next times: necessity to scan the EP badge.

After scanning their EP badge on the MFDs, the data subjects (users) have access to different parameters where they can choose to modify, print or delete files (previously sent to the printer) or to scan or copy files.

Anonymised data will be used for statistical purposes in order to have a better overview of the paper and toner consumption.

2.2 Indicate any legal basis (Treaty, Regulation, Decision, etc.) for this processing operation:

Article 5 (1.a) of Regulation (EU) 2018/1725 - Task carried out in the public interest or in the exercise of official authority vested in the Union institution or body.

2.3 Does this processing allow linkages between data processed for different purposes? ☐ yes ☒ no

2.4 Lawfulness: Indicate if

2.4.1 * ☒ the processing meets a functional need of the service

2.4.2 * ☐ the data subject has unambiguously consented to the processing

2.4.3 * ☐ any other basis, please specify

3. CATEGORIES OF DATA

'Personal data' means any information on an identified or identifiable natural person. Indicate all the categories of data contained in the file.

3.1 Categories of personal data

3.1.1	☐	data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct)	3.1.2	☐	concerning the data subject's family
3.1.3	☐	data relating to suspected offences, offences, criminal convictions or security measures	3.1.4	☐	concerning the data subject's career
3.1.5	☐	processing for the purpose of excluding individuals from a right, benefit or contract	3.1.6	☐	concerning leave and absences
3.1.7	☒	in the form of personal identification numbers	3.1.8	☐	concerning missions and journeys
3.1.9	☐	concerning the physical characteristics of persons as well as the image, voice or fingerprints	3.1.10	☐	concerning Social Security and pensions
3.1.11	☐	concerning the data subject's private sphere	3.1.12	☐	concerning expenses and medical benefits
3.1.13	☐	concerning pay, allowances and bank accounts	3.1.14	☒	concerning telephone numbers and communications
3.1.15	☐	concerning recruitment and contracts	3.1.16	☒	other

Civil status data and identification (First name, last name, badge number)
Data related to the professional sphere (Unit, Directorate, email)
Technical data (Windows user ID, password, username, technical job name [print, copy, scan job], date of the job and personal data included in the printing, copying and scanning data)

3.2 Special categories of data such as defined in Article 10 of Regulation EC n°45/2001

3.2.1	☐	revealing racial or ethnic origin	3.2.2	☐	revealing trade-union membership
3.2.3	☐	concerning political opinions	3.2.4	☐	concerning health
3.2.5	☐	revealing religious or philosophical beliefs	3.2.6	☐	concerning sex life

3.3 Please list the personal data processed

First name, last name, email, Unit, Directorate, badge number, Windows user ID, password, username, technical job name (print, copy, scan job), date of the job and personal data included in the printing, copying and scanning data.

4. DATA PROCESSING

'Data processing' means any operation carried out on personal data, whether or not by automated means.

4.1 Collection of data

4.1.1	☒	collection from the data subject (direct)	4.1.2	☒	other source of collection (indirect) - please specify

Personal data retrieved from the Active directory.
All information is imported via several LDAP connectors to the Active directory.

4.2 Processing of data

4.2.1	☒	processing automated wholly or in part
4.2.2	☐	non-automated processing of data intended to form part of a filing system
4.2.3	☐	manual processing of a structured set of data accessible according to given criteria

4.3 Storage of data

4.3.1 Indicate the period of storage and its justification:

For the printing, personal data are kept up in encrypted form to 96 hours since the creation of the printing jobs (when the files are sent to print). During this period, the retention period may be reduced depending on data subjects actions (delete, print, print + delete). => cf. Part 8 Further Info.
For the copying, personal data are kept in encrypted form on the multifunctional devices during the time of the copying process.
For the scanning, personal data are kept in encrypted form on the multifunctional devices during the time of the scanning process. Personal data are then transferred to the scan destinations chosen by the data subjects. The retention period for these transferred personal data are the ones established for each system of destination.
Encrypted records in databases (stored on European Parliament servers) are generated during the processing operations. Personal data will be retained for a maximum of 18 months from the moment they are collected.

4.3.2 Is any further processing for historical, statistical or scientific purposes envisaged? ☒ yes ☐ no

Indicate the form of storage used (anonymous, encrypted, other)

If it is required to retain the data after this period for statistics/analysis purposes, it will be anonymised.

4.3.3 Indicate the date or period of the beginning of the processing operations:

Autumn 2018

4.3.4 Indicate the date or period of the ending of the processing operations:

Not foreseen

4.4 File location

4.4.1 ☐ standalone PC

4.4.2 ☒ Parliament network. If the filing system is available on a network, indicate the location of the server:

// Data center (OPERATIONS)

4.4.3 ☐ interinstitutional network (indicate the institution(s) involved)

4.4.4 ☐ internet http://

4.4.5 ☐ intranet http://

4.4.6 ☐ other

5. RECIPIENTS & DATA TRANSFER

5.1 Recipients or categories of recipients to whom data are disclosed (physical or legal persons, administrations, companies, etc.):

Personal data are stored exclusively with restricted access on internal European Parliament servers. These personal data are accessible to the application owner (PRINTING Unit) and to a limited number of back-office staff members (OPERATIONS Unit).

If the data controller envisages transferring personal data, please answer the questions in this section.

5.2 In case of transfer within or between EU institutions or bodies:

N/A

5.2.1	Have the data been transferred following a request from the recipient?	☐ yes	☐ no
5.2.2	Has the data controller verified the competence of the recipient and made a provisional evaluation of the need for the transfer of the data?	☐ yes	☐ no
5.2.3	Has the recipient been informed of his obligations in respect of this transfer	☐ yes	☐ no

5.3 In case of transfer to recipients other than the EU institutions and bodies, subject to Directive 95/46/EC (e.g. national administrations, private sector):

N/A

5.3.1	Has the recipient established that the data are necessary?	☐ yes	☐ no
5.3.2	Has the recipient established the need for their transfer?	☐ yes	☐ no

5.4 In case of transfer to recipients outside the EU (please specify the legal basis, the nature of the data transmitted and their recipient):

N/A

5.4.1	Has the person responsible for the transfer established that an adequate level of protection is ensured in the country of the recipient?	☐ yes	☐ no

5.5 Is the transfer carried out by a sub-contractor? ☐ yes ☒ no

6. SECURITY OF PROCESSING

The data controller must implement the appropriate technical and organisational measures to ensure an appropriate security level with a view to the prevention of any unauthorised distribution or access, any accidental or illicit destruction, any accidental loss or deterioration, as well as any other form of illicit processing. Give a general description allowing a preliminary evaluation of the adequacy of the measures taken to ensure the security of processing

6.1 Physical security (access to computer systems, quality of the file supports, public access or restricted access to locations, storage, transport of equipment, etc.)

The new devices require user a physical authentication
When data subject (user) send files to print (job for printing) from a device (PC or mobile device), he/she can only collect his/her files after authentication.
Authentication process:
- First authentication: the user gives his/her credentials and badge number (by scanning it).
- Next authentications: the user gives only his/her badge number (by scanning it).
Servers storing personal data have a physical access strictly limited.
HDD Erase function: The HDD Data Erase will automatically overwrite and erase image data immediately after the job is completed; therefore, no trace of the data remains on the hard disk. It will perform an overwrite up to 3 times (DoD 5220.22M 3 pass) with random data for maximum security protection.

6.2 IT system(s) security (coding control, undue removal or transmission of data, passwords, encrypted directories, backup, audit trails for data processing and communication, etc.)

The HDD Data Encryption uses AES256-bit length encryption keys. This ensures that the data stored on the hard disk is protected against leakage of confidential information by theft of the hard disk.
Data are encrypted for the printing, scanning and copying.
Print server Spool file encryption protect files spooled to await on servers.
Encrypted Secure Print protect print jobs from being output at the device unattended.

6.3 Staff security (restricted access codes, conditions of subcontracting, etc.)

Concerning the accounting data in database (Statistics): accounting and reporting information are only available for the "Admin" ACL (Access Control List) group.

7. DATA SUBJECTS

The persons to be protected are identified or identifiable natural persons whose personal data are processed by the European Parliament in any context whatsoever.

7.1 Category (or categories) of data subjects (officials, other staff, contractors, European citizens, etc.):

- Officials
- Other internal staff (e.g. Trainees, Temporary agents)
- Contract agents
- MEPs
- APAs (Parliamentary Assistants)

7.2 Indicate the measures taken or envisaged to inform the data subject of the identity of the data controller, of any communication of data concerning him or her, and of his or her rights:

There are two communication tools to inform the data subject:
- Privacy Notice (on posters placed next to the printers and included in relevant intranet pages and emails of communication) notifying the data subjects of the processing of personal data and inviting them to see the Privacy Statement for further information on the processing.
- Privacy Statement (published on a dedicated intranet page) informing data subjects of all mandatory elements mentioned in Article 15 and 16 of Regulation (EU) 2018/1725.

7.3 Have any natural or legal persons employed by or under contract to the European Parliament received any instructions about confidentiality in processing personal data? ☒ yes ☐ no

7.4 Please explain how data subjects may exercise their rights (rights of access, of rectification, of blocking, of erasure and to object):

By sending an email to efficient_printing@ep.europa.eu.
Their requests will be analysed and processed.
Additional features have been requested (to the solutions' provider - Canon) in order to be able to reply to data subjects' requests.

7.5 If the processing operation is carried out by a processor, has a data protection clause been added in the contract? ☐ yes ☐ no

8. FURTHER INFORMATION

Give any information you consider relevant and indicate the heading it refers to:

In 4.1.1:
During the authentication process, the user gives his/her credentials and badge number (first authentication) then only his/her badge number (next authentications).
The badge number is given by just scanning the badge on the dedicated zone of the device.
Then the data subject has the possibility to insert, modify and delete a file or a configuration.

In 4.3.1 (one clarification):
For the printing, personal data are kept up in encrypted form to 96 hours since the creation of the printing jobs (when the files are sent to print). During this period, the data subjects have the possibility on the multifunctional devices:
-To delete files to print (in this case personal data are automatically deleted).
-To print files (in this case personal data are moved in the “Printed Jobs” tab and deleted at the end of the 96 hours).
-To print and delete files via the feature “Print + Delete” available in the “Options” window (in this case personal data are automatically deleted).

Pursuant to Article 26 of Regulation (EC) 45/2001, the information given above is, except for item 6, intended to appear in the register of the notified personal data processing operations of the European Parliament. This register, placed by this Regulation under the responsibility of the Data Protection Officer of the European Parliament, is intended for public information to ensure that data subjects may ascertain the existence of filing systems containing personal data, in order to enable them to exercise their rights in accordance with that Regulation. Any person may consult the register directly or indirectly though the European Data Protection Supervisor. The data controller is required to provide all the information requested by the Data Protection Officer and has a right of access to and rectification of these data. Data appearing in this register will be preserved for the duration necessary for the accomplishment of the purpose for which they have been collected. Any data subject and any person employed by an institution or Community body may lodge a complaint with the European Data Protection Supervisor for violation of the Regulation, and may bring an action before the Court of Justice of the European Communities. Any failure to comply with obligations pursuant to the Regulation, whether intentionally or through negligence makes an official or other servant liable to disciplinary action.

The data controller declares the accuracy of the above statements and undertakes to notify any change affecting this information to the Data Protection Officer of the European Parliament.

Date: Signature of data controller

See the instructions at the bottom of this notification

---

* The signed notification is to be sent within 10 days to the Data Protection Officer of the European Parliament, KAD 02G028, Luxembourg

* For further information please consult the intranet site of the European Parliament

http://www.epintranet.ep.parl.union.eu/intranet/ep/lang/en/content/administrative_life/personnel/data_protection_1/

or write to: Data-Protection@europarl.europa.eu