Data Protection - DG ITEC Record of processing activity

Description of personal data processing

Purpose: This file presents a detailed description of a personal data processing. Such description has to be included in the Record file in the context of the Accountability principle laid down in Article 4(2) of Regulation (EU) 2018/1725.

By signing this document, the Data Controller of the processing declares the accuracy of the statements and undertakes to update any change affecting this information.

Please refer to Article 31 of Regulation (EU) 2018/1725 presenting the requirements on Records of processing activities.

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.	
First name	[redacted]
Last name	[redacted]
E-mail	[redacted]
Function	Head of Unit
Administrative Address: Building and room	[redacted]
Tel.	[redacted]
Place of work	Luxembourg
The joint controller is the unit or other organisational entity which, jointly with other data controller(s), determines the purposes and means of the processing of personal data.	
Name and contact details of joint controller (where applicable)	
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 (under Directorate for Publishing & Distribution)
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 internal decision or initiative for this processing operation	These ePrinters are installed to meet the objectives of the Parliamentary Project [ITEC P12] "Efficient printing" presented in the Parliamentary Project Portfolio (PPP) implementing the SEF (Strategic Execution Framework) 2017-2019.	
2.3 Does this processing allow linkages between data processed for different purposes? (Compatible purposes)	YES: ☐ NO: ☒	If YES, please specify:
2.4 Lawfulness:	☒ Article 5 (1.a) - Task carried out in the public interest or in the exercise of official authority vested in the Union institution or body *Remark: It shall be laid down in Union Law*	
	☐ Article 5 (1.b) - Legal obligation to which the data controller is subject *Remark: It shall be laid down in Union Law*	
	☐ Article 5 (1.c) - Performance of contract (specific choice of data subjects)	
	☐ Article 5 (1.d) - Data subjects' consents - freely given, specific, informed and unambiguous (clear affirmative action from data subject)	
	☐ Article 5 (1.e) - Protect the vital interest	
	☐ 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	Civil status data and identification	☒ First name and last name ☐ Photography ☐ Citizenship(s) ☐ Identification card number ☐ Sex ☐ Date and place of birth ☐ Other (please specify below in the “Other” part)
	Data related to the professional sphere	☐ Data about recruitment ☐ Office number ☐ Phone number

		☒ Directorate, Unit, Service, Department ☒ Email address such as name.surname@xxx.yyy ☐ Communication ☐ Employee number ☐ Job title (especially if it is unique) ☐ Training, skills, degree and certification ☐ Employee's work ☐ Ability, efficiency, conduct ☐ Employment contract and salary ☐ Leave and absence ☐ Missions / journeys ☐ Career ☐ Suspected offences, offences, criminal convictions or security measures ☐ Other (please specify below in the "Other" part)
	Data related to the private sphere	☐ Home address (street, zip, postal code, city) ☐ Phone number ☐ Email address such as name.surname@xxx.yyy ☐ Bank account / credit card number ☐ Habits of life ☐ Family situation or concerning the data subject's family ☐ Social security and pensions ☐ Income, financial, fiscal situation ☐ Suspected offences, offences, criminal convictions or security measures ☐ Other (please specify below in the "Other" part)
	Technical data	☒ Identifier (e.g. login) ☒ Username ☐ Location data ☐ Internet Protocol (IP) address ☐ MAC address ☐ Cookie ID ☐ Other (please specify below in the "Other" part)
	Other (e.g. other physical characteristics) - Please specify:	Badge number, technical job name of the job (scan, print, copy), date of the job, personal data included in the printing, copying and scanning data.
3.2 Special categories of personal data	☐ Revealing racial or ethnic origin ☐ Revealing political opinions ☐ Revealing religious or philosophical beliefs ☐ Revealing trade union membership ☐ Processing of genetic data ☐ Processing of biometric data for the purpose of uniquely identifying a natural person ☐ Processing of data concerning health ☐ Processing of data concerning a natural person's sex life or sexual orientation	
3.3 Please list the personal data processed	First name, last name, Unit, Directorate, email, unit, 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	☒ Collection from the data subject (direct) - please specify:	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.
	☒ 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	☒ Processing automated wholly or in part ☐ Non-automated processing of data intended to form part of a filing system ☐ 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:	**On the current archives:** **- 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 the files to print (in this case personal data are automatically deleted). • To print the 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 the files via the feature "Print + Delete" available in the "Options" window (in this case personal data are automatically deleted). **- 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. **On the intermediate archives:** **- 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. In case of investigation, personal data may be kept for a longer time necessary to conduct the investigation.
	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	☐ Standalone PC ☒ Parliament network --> If the filling system is available on a network, please indicate the location of the server: // Data center (OPERATIONS) ☐ Interinstitutional network (indicate the institution(s) involved) ☐ Internet http:// ☐ Intranet http:// ☐ Other:	

5. RECIPIENTS & DATA TRANSFER

5.1 Recipients or categories of recipients to whom data are or will be disclosed *(physical or legal persons, administration, companies, staff under the controller or another service within EP, 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 (or has already transferred) personal data, please answer the questions in this section.* ** The Regulation (EU) 2018/1725 came into force on the 11th of December 2018. This record presents the characteristics of processing operations processed since the coming into force of this Regulation (since the 11/12/2018).The previous period is not considered here.*			Specify (if necessary) the rows below:
5.2 Are there transfers foreseen (or already made) within or between EU institutions or bodies? YES: ☐ NO: ☒	5.2.1 [Will/Have] the data [be/been] transferred following a request from the recipient?	N/A	
	5.2.2 [Will/Has] the data controller [have the possibility to verify/verified] the competence of the recipient and [to make/made] a provisional evaluation of the need for the transfer of the data?	N/A	
	5.2.3 [Will/Has] the recipient [be/been] informed of his obligations in respect of this transfer?	N/A	
5.3 Are there transfers foreseen (or already made) to recipients other than the EU institutions and bodies (e.g. national administrations, private sector)? YES: ☐ NO: ☒	5.3.1 Has the recipient established that the data are necessary?	N/A	
	5.3.2 Has the recipient established the need for their transfer?	N/A	
5.4 Are there transfers foreseen (or already made) to recipients outside the EU	Please specify the legal basis, the nature of the data that [may be/were] transmitted and their recipient:	N/A	

(e.g. third countries or international organisations)? YES: ☐ NO: ☒	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?	☐ Adequacy decision by the EC ☐ International agreement ☐ Appropriate safeguards *(e.g. standard data protection clauses adopted by the EC or the EDPS; contractual clauses or provisions authorised by EDPS)* ☐ Derogations for specific situations *(e.g. protect vital interests; important reasons of public interest; establishment, exercise or defence of legal claims)*

6. SECURITY

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 internal staff (e.g. Trainees, Temporary agents) ☒ Contract agents ☒ MEPs ☒ APAs (Parliamentary Assistant) ☐ European citizens ☐ Visitor of the European Parliament ☐ Other, please specify:	
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 Processor	Is the processing operation carried out by a processor?	YES: ☐ NO: ☒
	If "YES": Has a data protection clause been added in the contract?	N/A

8. FURTHER INFORMATION

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

The data controller declares the accuracy of the above statements and undertakes to update any change affecting this information.

Signature of the data controller: