Directorate General: Innovation and Technological Support (DG ITEC)

High-risk pre-assessment

[on MFDs - Multifunctional devices]

Purpose: This document presents the high-risk pre-assessment (or "threshold assessment") performed as a prior analysis to decide if it is necessary to carry out a DPIA (Data Protection Impact Assessment) under Article 39 of the EU-DPR (Regulation [EU] 2018/1725).

Name of the processing operation: Multifunctional devices for printing, copying and scanning with authentication process

Entity of the data controller in practice: DG ITEC/EDIT/Printing Unit

Date of the high-risk pre-assessment: 01/10/2019

1. DETERMINATION OF APPLICABILITY OF AN EXCLUSION OR DEROGATION FROM CONDUCTING A DPIA

Description of derogation	*Yes / No*
DPIA already carried out as a part of general impact assessment Does the processing have a legal basis in a legal act adopted on the basis of the Treaties, which regulates the specific processing operation or set of operations in question, and where a DPIA has already been carried out as part of a general impact assessment preceding the adoption of that legal act and is done pursuant to point (a) or (b) of Article 5(1)?	NO
DPIA carried out for a similar processing operation Was a DPIA carried out for a similar processing operation that presents similar high risks?	NO
EDPS list of processing operations prima facie not requiring DPIA Does the processing activity correspond to any of the processing activities on this list?	NO
- Management of personal files under Article 26 of the Staff Regulation as such* **some procedures resulting in adding information to the personal file may require DPIAs, but not the repository of personal data as such.*	NO
- Standard staff evaluation procedures under the Staff Regulation (annual appraisal)	NO
- Standard 360° evaluations for helping staff members developing training plans	NO
- Standard staff selection procedures	NO
- Establishment of rights upon entry into service	NO
- Management of leave, flexitime and teleworking	NO
- Standard access control systems (non-biometric*) **e.g. badges to be swiped at entry points.*	NO
- Standard CCTV on a limited scale (no facial recognition, coverage limited to entry/exit points, only on-premises, not in publicly accessible space)	NO

2. INDICATORS FOR HIGH RISKS

Do the processing operations present any of the characteristics mentioned below?	*Yes [If so, describe] / No [if borderline: why not?]*	Justification
1. Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting. *Examples:* *- a bank screening transactions in accordance with applicable law to detect possibly fraudulent transactions;* *- profiling staff based on their transactions in a case management system with automatic reassignment of tasks.* *Counterexamples: standard appraisal interviews, voluntary 360° evaluations for helping staff to develop training plans.*	NO	For the individual statistics [coming features], the multifunctional devices (MFDs) only store metadata on consumption (not the content of the documents) that will be made available for consultation to each individual user. These statistics will not refer to the performance of the user. The goal is to encourage each user (data subject) to reduce his/her impact on the environment. Such data will be reported (for consultation purposes) only to the concerned user (data subject) via a specific web portal accessible upon authentication.
2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects. *Example: automated staff appraisal ('if you're in the lowest 10% of the team for the number of cases dealt with, you'll receive a "unsatisfactory" in your appraisal, no discussion').* *Counterexample: a news site showing articles in an order based on past visits of the user.*	NO	/
3. Systematic monitoring: processing used to observe, monitor or control data subjects, especially in publicly accessible spaces. This may cover video-surveillance but also other monitoring, e.g. of internet use. *Examples: covert CCTV, smart CCTV in publicly accessible spaces, data loss prevention tools breaking SSL encryption, tracking movements via location data.* *Counterexample*: open CCTV of garage entry not covering public space.	NO	/
***4.* Sensitive data or data of a highly personal nature**: data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for uniquely identification purposes, data concerning health or sex life or sexual orientation, criminal convictions or offences and related security measures or data of highly personal nature. *Examples: pre-recruitment medical exams and criminal records checks, administrative investigations & disciplinary* proceedings, any use of 1:n biometric identification. *Counterexample: photos are not sensitive as such (only when coupled with facial recognition / biometrics or used to infer other sensitive data).*	NO	Different natures of personal data (present in the documents to be printed, copied and/or scanned) may be processed in the MFDs in order to print/scan/copy the documents themselves. However, the MFDs do not analyse the content of the documents, do not store the content of the documents scanned/copied and do not store longer than 96 hours the content of the documents printed or to be printed (time where the data subject can launch or relaunch the print job(s) of his/her documents).

5. Data processed on a large scale, whether based on number of people concerned and/or amount of data processed about each of them and/or permanence and/or geographical coverage. *Examples: European databases on disease surveillance* *Counterexample: invalidity procedures under Article 78 of the Staff Regulations in a medium-sized EUI.* => The following factors should be considered: a. the number of data subjects concerned; b. the volume of data being processed; c. the duration/permanence, of the data processing activity; d. the geographical extent of the processing activity.	YES	Number of data subjects: ++++ (they are persons entitled to consume the European Parliament printing / scanning / copying services, such as the MEPs and APAs, the EP/Other EUIs officials, the EP/Other EUIs temporary and contract agents, the EP/Other EUIs trainees) Volume of data: ++++ (a lot of documents are processed in order to print/scan/copy the documents themselves) Period of retention: ++ (content of the documents are not stored longer than 96 hours, metadata on consumption are kept until 18 months) Geo. extent: + (the processing is performed in the EU territory mainly in Brussels, Strasbourg, Luxembourg and also in certain agencies)
6. Datasets matched or combined from different data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject. *Example: cross-checking access control data and self-declared working hours following a suspicion of fraudulent declarations in an administrative inquiry (following the applicable rules).* *Counterexample: further use of data processed for a grant application when auditing the grant process.*	NO	Personal data are stored exclusively with restricted access on internal European Parliament servers. These personal data are accessible to the application owner (ITEC - PRINTING Unit). A limited number of back-office staff members (ITEC - OPERATIONS Unit) may receive (if necessary, i.e. for support/debugging purposes) log files. The user (data subject) will have access to his/her statistics.
7. Data concerning vulnerable data subjects: situations where an imbalance in the relationship between the position of the data subject and the controller can be identified. *Examples: children, asylum seekers, mentally ill persons* *Counterexample: delegates in a Council Working Party (for attendance lists), members of expert groups (for travel cost reimbursement)*	NO	The MFDs provides support for the employees/MEPs to execute basic and necessary tasks in the context of their work relationship/mandate.
***8.* Innovative use or applying technological or organisational solutions** that can involve novel forms of data collection and usage. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. *Examples: machine learning, connected cars, combining use of finger print and face recognition for improved physical access control, social media screening of job applicants..* *Counterexample: 1:1 biometric access control using fingerprints* => The use of a new technology, defined in "accordance with the achieved state of technological knowledge" can trigger the need to carry out a DPIA.	NO	/

9. Preventing data subjects from exercising a right or using a service or a contract. *Examples: exclusion databases, credit screening* *Counterexample: determination of rights upon entry into service (e.g. expatriation or dependent child allowances).*	NO	For the individual statistics [coming features], the goal is to encourage each user (data subject) to reduce his/her impact on the environment. Such data will be reported (for consultation purposes) only to the concerned user (data subject) via a specific web portal accessible upon authentication. These statistics will not refer to the performance of the user. The user will not be blacklisted.
10. **Data transfer to recipients outside the EU/EEA** *Examples: outsourcing to companies outside the EU/EEA; structured cooperation with an international organisation leading to the exchange of personal data.*	NO	/

3. DETERMINATION OF APPLICABILITY OF AN OBLIGATION TO CONDUCT A DPIA

Description of obligation	*Yes / No*
EDPS list of processing operations prima facie requiring DPIA (EDPS decision of 16/07/2019) Does the processing activity correspond to any of the processing activities in this list?	NO
- Exclusion data bases [cf. indicators 2, 4, 9]	NO
- Large-scale processing of special categories of personal data (such as disease surveillance, pharmacovigilance, central databases for law-enforcement cooperation) [cf. indicators 1, 4, 5, 8]	NO
- Internet traffic analysis breaking encryption (data loss prevention tools) [cf. indicators 1, 3, 8]	NO
- E-recruitment tools automatically pre-selecting/excluding candidates without human intervention [cf. indicators 1, 2, 8]	NO

4. CONCLUSION

Number of "Yes" ticked above	**1**	Justification
A DPIA is not required as one or more from the derogations mentioned above apply (section II)	NO	/
A DPIA is required as one or more from the obligations mentioned above apply (section III)	NO	/
Final assessment: If you have two or more "YES" in the list of indicators above, you should carry out a DPIA. - If you consider that in the specific case at hand, risks are not "high" even though you have two or more "yes", explain and justify why you think the processing is in fact not "high risky". - If you consider that in the specific case at hand, risks are "high" even though you have less than two "yes", explain and justify why you think the processing is in fact "high risky".	NO	The MFDs process on a large-scale personal data, but it is normal due to the context and purpose of the processing. Indeed, the MFDs support for the employees/MEPs to execute basic and necessary tasks in the context of their work relationship/mandate. The MFDs do not analyse the content of documents, do not store documents scanned/copied and do not store longer than 96 hours the content of the documents printed or to be printed (time where the data subject can launch or relaunch the print job(s) of his/her documents). The MFDs record metadata on printing consumption (per machine assigned to an entity), and soon per user [coming features] to raise awareness on the environmental impact (EMAS objective). The individual statistics [coming features] will be made available for consultation to each individual user. These statistics will not refer to the performance of the user. The goal is to encourage each user (data subject) to reduce his/her impact on the environment. Such data will be reported (for consultation purposes) only to the concerned user (data subject) via a specific web portal accessible upon authentication.