From: [redacted]
Sent: 24 October 2019 19:56
To: [redacted]
Cc: [redacted] European Data Protection Supervisor; [redacted]
Subject: RE: Request for information | 2019-0373
Attachments: Att 1 - Description of the processing - C_1 - MFDs.pdf; Att 2 - Description of the processing - C_1 - MFDs (signed).pdf; Att 3 - High risk pre-assessment DG ITEC - MFDs.pdf; Att 4 - 2019.10.11 - DPS - MFDs with authentication process.pdf; Att 5 - 2019.10.11 - DPN - MFDs with authentication process.pdf; Att 6 - Request to update the declaration within the DPO register.pdf

Dear [redacted]

First of all, thank you for the recommendations presented in your last email dated 26/07/2019. DG ITEC has taken note of the different points raised and analysed carefully the way to implement actions to meet the recommendations.

In this e-mail we will present **the current state of play on the measures implemented and planned**. We would also like take the opportunity to clarify the information previously provided and to explain future developments foreseen for the processing.

The multifunctional devices (MFDs) were 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. This project is going to evolve into a new Parliamentary Project "Needs-based printing in the digital age" presented in the Parliamentary Project Portfolio (PPP) implementing the SEF (Strategic Execution Framework) 2019-2021.

The objective is to reduce printing in the digital age. A key element of this project is to raise awareness at the individual level to meet the EMAS objectives on the reduction of paper and toner consumption hence to raise awareness on environmental impacts. Through this means, we expect to encourage users (data subjects) to reduce their impact on the environment when executing tasks in the context of their work relationship/mandate.

Please find below the requested answers and clarifications:

Retention period

Please refer to the point 4.3 of the Record and/or the section "How long are the personal data kept?" of the Data Protection Statement (attached).

- Our services reviewed the retention periods rules in order to cover the different services managed by the multifunctional devices (MFDs) and to assess the future functionality related to the individual statistics on printing.

- As regards **the authentication process**:
  Personal data (i.e. Windows user ID, first name, last name, email) are synchronized (i.e. continuously collected and so updated [creation/erasure]) with the Windows directory services (corporate directory).

- On **the content of documents**:
  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 (this time is to allow the data subject can launch or relaunch the print job(s) of his/her documents).

- **Concerning the activity logs used to produce global and individual statistics on printing processing operations:**
  - Records in databases are generated during the printing operations. These records include personal data only about paper and ink consumption (not on document content).
  - They are used for the global statistics (per machine assigned per entity).
  - They will be used for individual statistics on consumption (available for consultation purposes only to the concerned user).
    The individual statistics on consumption are in development. The users (data subjects) will be informed prior to the activation of this new feature. The individual statistics will be presented to the users via the provision of a user dashboard and/or user notifications. The purpose of this being to raise awareness on the user's individual impact on the environment. These records will be retained for a maximum of 18 months from the moment they are collected. Statistics will cover a sufficient period to present at least two scenarios of the same context and be able to compare these scenarios.

- **On the activity logs used for support/debugging purposes**:
  - There are different levels of logging available. In normal conditions, neither user information nor job information is recorded. However, at maximum level of logging (to debug an issue), the user identifier, the user name, the technical job identifier and the technical job name may be recorded depending on the nature of the issue.
  - All type of logs are kept for 30 days, except in case of an error where data are deleted after the issue is resolved or after 1 year if it comes first.
  - In case of an investigation (foreseen in the applicable Regulations to the EUIs and Internal Rules), the same retention period rules will apply. Personal data will be transferred directly to the competent authority for the investigation managing the relevant processing operation. They will apply the retention rules applicable to the purpose of their processing operation, which will be then out of the scope of DG ITEC.

Data protection notice publication

- DG ITEC assessed different tools to provide the data subjects with updated information regarding the processing of their personal data. In this respect, there are ongoing discussions and tests with Canon (solution provider) to implement a functionality to present the full Data Protection Statement (via the MFDs) to the users (data subjects) prior to using the MFDs. This involves requesting an additional feature to the provider.
- As the project evolves, a new version of the Record adapted to the new features will be created and signed. Based on the elements declared in the Record, two communication tools will be presented to inform the data subject:
  - Data Protection Notices notifying the data subjects of the processing of personal data and inviting them to see the Data Protection Statement for further information on the processing (to be presented at least on the poster next to each machine and on the intranet pages presented the MFDs)
  - Data Protection Statement informing data subjects of all mandatory elements defined in Article 15 and Article 16 of Regulation (EU) 2018/1725 (to be presented at least on the intranet, on the user manual and in the MFDs).

- Finally, a communication campaign will be launched to inform the data subjects proactively on the processing of their personal data when using the printers and to present the upcoming functionalities related to the individual statistics.

Controller-Processor relationship

- As presented in the Record, the European Parliament is the data controller. Due to security rules imposed by the European Parliament, Canon does not have access and cannot use the personal data. For this reason it is considered as a solution provider (software and hardware).
- DG ITEC sends only statistics per machine (without personal data) to Canon (e.g. for billing purposes).
- The MFDs use the Neevia application, set up and used locally (not connected), to convert documents into spool files. Neevia does not have access or cannot use the personal data, and is therefore considered as a software provider.

Technical and organisational measures

a. Data protection by design and by default:

- In order to comply with the obligation related to the Data protection by design and by default, the data controller in practice has included in the project cycles the notion of high-risk pre-assessment. Also called threshold assessment, it is 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).

- Please refer to the High-risk pre-assessment (threshold assessment) attached to this email.

  The results of this high-risk pre-assessment are as follows:
  1. Determination of applicability of an exclusion or derogation from conducting a DPIA
     - Result: No exclusion or derogation applicable.
  2. Indicators for high risks
     - Result: 1 indicator of high-risk is present in the processing (data processed on a large scale)
  3. Determination of applicability of an obligation to conduct a DPIA
     - Result: No obligation applicable
  4. Conclusion presenting the final assessment taking into account the 3 previous parts
     - Result: 1 indicator of high-risk is present in the processing (data processed on a large scale). Furthermore, this type of risk is accepted due to the context and purpose of the processing. Indeed, the MFDs support for the data subjects to execute basic and necessary tasks in the context of their work relationship/mandate.
- Therefore, no high-risks have been identified following this High-risk pre-assessment. However, an assessment will have to be conducted again every time there is a change on the MFDs that may have an impact for the data subjects.

b. General safeguards

- During the first connection with the MFDs, the data subject has to register the EP badge that will be linked to his/her MDFs account (ID and password from the EP LDAP are required).
  The login data (i.e. Windows user ID, first name, last name, email) are then synchronized (i.e. continuously collected and so updated) with the Windows directory services (corporate directory) to ensure a secure authentication process.

- Thus, if there is a the loss or the theft of a badge, the data subject can inform the HelpDesk that will notify directly DG SAFE, which will deactivate or block the badge without delay. The MFDs systems do not accept a deactivated or blocked badge. DG SAFE launches immediately the process to create a new badge when they are notified of loss or theft of a badge. The badge of the data subject will be linked directly to his/her new MDFs account. He/she will need to restart the authentication process (first authentication).

c. Encryption

- The HDD Data Encryption uses AES256-bit length encryption keys. This ensures that the data stored on the hard disk are protected against leakage of confidential information by theft of the hard disk.
- Data are encrypted for the printing, scanning and copying. The end-to-end encryption will depend on all terminals used:
  - The MFDs are all encrypted.
  - The EP servers used in the solution are all encrypted. The print server spool file encryption protects files spooled to await on servers.
  - The terminal of the user (i.e. if the PC, mobile phone, tablet [sending the document to be printed or receiving the document scanning]), knowing that
    - The corporate terminals are all encrypted (desktop, laptop, hybrid)
    - The personal devices cannot be connected to UniFlow (MFDs software solution).

I hope these clarifications are useful, do not hesitate should you have any question or need further clarification.

[redacted]

Data Protection Coordinator DG ITEC

[redacted]

European Parliament

Directorate-General for Innovation and Technological Support
[redacted]
www.europarl.europa.eu

From: [redacted]
Sent: 01 August 2019 07:55
To: [redacted]
Cc: [redacted] ; European Data Protection Supervisor
Subject: RE: Request for information | 2019-0373

Dear [redacted]

Thank you very much for your analysis and recommendations.
On behalf of Maria Castillejo, I acknowledge receipt of your email dated 26 July 2019.
We will analyse it and provide you with a reply within three months as presented in your conclusion.

Yours sincerely,

[redacted]

European Parliament
Innovation and Technological Support
Innovation and Resources
Innovation, Performance and Internal Control

[redacted]
www.europarl.europa.eu

From: [redacted]
Sent: 26 July 2019 18:08
To: [redacted]
Cc: [redacted]; European Data Protection Supervisor ; [redacted]
Subject: RE: Request for information | 2019-0373
Importance: High

Dear [redacted]

We are writing to you concerning the EDPS informal consultation, opened on 16 April 2019, on the data processing regarding the European Parliament's (EP) 'efficient printing' system.

On September 2018, the EP announced the implementation of an 'efficient printing' system, which requires the EU staff to use their badge and introduce their computers user name and password, implying a personal data processing. On 8 February 2019, a complaint (case 2019-0149) was filed regarding the implementation of this 'efficient printing' system. It was agreed with the complainant to close the complaint provided that the EDPS follow-up the issue with a consultation.

After a meeting between the EDPS and EP staff on 4 April 2019, as well as subsequent exchange of information, the EDPS has analysed the data processing regarding the 'efficient printing' system.

I. Legal analysis and recommendations

This informal consultation analyses and highlights only those practices which do not seem to comply with the principles of the Regulation (EC) 2018/1725 (hereinafter 'the Regulation').

Retention period

According to the information provided, the data related to the user of the printer (e.g. user badge number, username, email address, printing job, etc.) will be stored in an encrypted form for 96 hours on the "current archives" following the creation of the printing jobs.

In addition, these data will be stored up to 18 months in an encrypted form in an EP server (the intermediate archive). In case of an investigation, personal data may be kept for a longer period.

Except if there is an on-going investigation on a concrete case, the EP has not provided factual elements that justify the retention of data for more than 96 hours. Additionally, the EDPS believes that storing all the printing and scanning information – which may contain personal data of the users – for 18 months is excessive.

Therefore, as a **general rule** and unless the EP provides additional arguments on this issue, we recommend that the **maximum retention period be 96 hours.** In the event of specific EU staff members being under investigation, the retention period can be extended until the completion of the investigation to preserve the evidence. However, this exception should be duly justified and documented.

2. Data protection notice publication

The EP published a data protection notice regarding this processing on the Intranet. After considering other possibilities – such as the data protection notice being displayed on posters close to the printers – the EP questioned the feasibility of those measures and requested advice from the EDPS.

The data protection notices should be visible to all data subjects prior to using the printing service. In that sense, the EDPS recommends that the **EP actively**

inform data subjects. One possibility would be to display a data protection notice next to all printers. This way, the users will be able to read it and be informed before submitting their credentials. Other possibilities might be an e-mail to all staff informing them (for existing users); for newcomers, the EP could do this as part of their welcome package or by showing the notice on the printer's screen when a new badge is used the first time.

3. Controller-Processor relationship

According to the information provided and to our understanding, the EP is the controller and Canon is a processor in this data processing since they are processing data on behalf of the controller. However, this relationship is not reflected in the data protection records. Hence, we recommend that the **records be amended**, in order to include this controller–processor relationship.

In this regard, we would like to remind the EP that data processing by a processor shall be governed by a contract or other legal act, in accordance with Article 29(3) of the Regulation and the EDPS assume that the EP has signed such agreement (which includes strong provisions in relation to data protection) with all its processors involved in this printing system.

Additionally, the involvement of Neevia is also mentioned in the data processing flowcharts submitted to the EDPS, but the limited information provided does not allow us to assess if Neevia is a processor or a mere software provider. Therefore, we suggest that the EP analyse the role of Neevia in this data processing and adopt the necessary steps following that analysis to ensure full compliance with the Regulation.

Furthermore, we would like to highlight that one of the responsibilities of the controller is to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures, in accordance with Article 29 of the Regulation.

4. Technical and organisational measures

a. Data protection by design and by default

Article 27 of the Regulation creates a new obligation in comparison to the previous data protection framework: data protection by design and by default. This means that the controller has to implement appropriate technical and organisational measures during both the development and the use of a data processing. This obligation exists independently of the obligation to conduct a data protection impact assessment (DPIA) in some cases.[1] In order to comply with the requirements of data protection by design and by default, the EP should perform a risk assessment that addresses the vulnerabilities and potential risks to the data subjects.

In this regard, data protection by design and by default also requires that the EP implement appropriate technical and organisational measures and safeguards on its servers and that special attention is paid not only the software installation, but also to future updates.

b. General safeguards

According to the information provided, this 'efficient printing' system is stored exclusively on internal EP servers with restricted access.

From the information provided, it is not clear how the EP links the badge ID and the user sessions for authentication in a request to print/scan a document. It is for the EP to ensure that any personal data processed here is minimised in accordance with the principle of data protection by design and by default.

Regarding the security measures, please note that some of the printed or scanned documents may contain special categories of data, whose unauthorised disclosure may cause significant harm to data subjects. We were not provided with enough information to make a global assessment, but we trust that the EP is aware of the sensitivity of the information at issue and that the necessary technical and organisational security measures are being adopted.

Moreover, the information provided does not state whether the EP assessed the threat of lost/stolen badges being used to retrieve pending print jobs. We suggest that the EP assess this risk, and if necessary, establish a quick procedure to block printing for lost or stolen badges.

c. Encryption

As it is presented in the description of the processing, the HDD Data Encryption (using AES 256-bit encryption) protects data stored on the hard disk in the server.

According to the information provided, '… the Canon solution (uniFLOW) also uses AES 256-bit encryption to protect print job data while in transmission over the network. To protect print jobs from being output from an unattended device, the encrypted secured printing feature holds the job in a queue until the user releases the job using one of the agreed authentication methods'.

The document is sent to the server without being encrypted. Then, it is encrypted. Encrypting the document using **end-to-end encryption** before sending it to the server would be safer. **We do not know whether the EP assessed this point in its information security risk assessment for the 'efficient printing' system and would recommend that it do so if it has not done so.**.

II. Conclusion

We believe that if the EP effectively implements all the recommendations mentioned above, there is no reason to believe the EP data protection safeguards regarding the 'efficient printing' system are not appropriate.

Please inform the EDPS about the implementation of the above recommendations with the documentary evidence thereof within **three months** of the date of this message.

Please note that this is informal advice at staff level and does not prejudice any formal position that the EDPS might take. Should you need a formal reply (letter signed by Head of Unit or Supervisor), we can arrange that as well, but please note that it may take longer.

[1] The EDPS has issued a list of data processing subject to the DPIA obligation under Article 39(4) of the Regulation. Prima facie, it appears the 'efficient printing' system would not fall under this obligation. The list is available at: https://edps.europa.eu/data-protection/our-work/publications/guidelines/data-protection-impact-assessment-list_en.

Yours sincerely,

[redacted]

European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels

Office address: Rue Montoyer 30, B-1000 Brussels
@EU_EDPS www.edps.europa.eu

From: [redacted]
Sent: 12 July 2019 15:56
To: [redacted]
Cc: [redacted] European Data Protection Supervisor <EDPS@edps.europa.eu>; [redacted]
Subject: RE: Request for information | 2019-0373

Dear [redacted],
We are pleased to share with you data flow diagrams that we received from Canon.
These diagrams present data management per process: Logon process, End-user Print and Release, Mobile Print, Scanning process, Logoff process, Communication between each server and MFD.
Please also find attached a glossary on the technical terms used.
I hope these elements will provide you with sufficient information for the analysis.
Please, do not hesitate should you have any question or need further clarification.
Kind regards,

[redacted]
European Parliament
Directorate-General for Innovation and Technological Support
[redacted]
www.europarl.europa.eu

From: [redacted]
Sent: 08 July 2019 15:33
To: [redacted]
Cc: [redacted]; European Data Protection Supervisor ; [redacted]
Subject: RE: Request for information | 2019-0373
Dear [redacted]
In your previous correspondence you have said that 'The application owner is in contact with the solution provider (Canon) to obtain a complete diagram of the data flow of the ePrinting system'.
In our view, this information is very important to the analysis of this case file.
Therefore, in case you have received it, could you please provide us with that data flow diagram?
In case you have not yet received it, could you please inform us when are you expecting to receive that information?
Thank you in advance for your cooperation.
Kind regards,
[redacted]

From: [redacted]
Sent: 11 June 2019 19:03
To: [redacted]
Cc: [redacted] European Data Protection Supervisor <EDPS@edps.europa.eu>; [redacted]
Subject: RE: Request for information | 2019-0373
Dear [redacted]
Thank you very much for your reply. We will analyse it and provide you with feedback asap.
Kind regards,
[redacted]

From: [redacted]
Sent: 11 June 2019 18:37
To: [redacted]
Cc: [redacted]; European Data Protection Supervisor ; [redacted]
Subject: RE: Request for information | 2019-0373
Dear [redacted]
Thank you for your attention to the analysis of the document presented. We are pleased to answer your questions with the following explanations per point raised.

1. Anonymous data

The statistics carried out are based on standard requests where anonymous results have a minimum level of granularity per machine assigned to an organisational entity (e.g. a Directorate, a Unit, a Service). The data processed are the number and type of printed pages, the colorimetric mode (color, black and white) and the printing date. These are global statistics used to determine the most appropriate allocation of printing resources in terms of paper and printer cartridges.
Please find attached some examples of these global statistics.

2. Complete diagram of the data flow

The application owner is in contact with the solution provider (Canon) to obtain a complete diagram of the data flow of the ePrinting system.

3. Data retention

We mentioned 18 months since we were aware of an existing script exchanged with the European Commission to reduce

the data retention period. However, we need now to reconsider this retention period since we have recently received a request from the Directorate-General for Personnel (DG PERS) of the European Parliament to keep personal data for a longer period to be used in inquiries and disciplinary cases. In the context of Article 86 of the Staff Regulations (and their Annex IX) and the general implementing provisions governing disciplinary proceedings and administrative investigations, DG PERS would propose the retention period of the discharge plus two years, given that no retention period is foreseen in those legal basis.
Your advice on this would be very useful.

4. Data encryption

As it is presented in the description of the processing, the HDD Data Encryption (using AES256-bit encryption) protects data stored on the hard disk.
At the software level, the Canon solution (uniFLOW) also uses AES 256-bit encryption to protect print job data while in transmission over the network. To protect print jobs from being output from an unattended device, the encrypted secured printing feature holds the job in a queue until the user releases the job using one of the agreed authentication methods.
I hope these clarifications are useful, do not hesitate should you have any question or need further clarification.
Maria Castillejo

[redacted]
European Parliament
Directorate-General for Innovation and Technological Support
[redacted]
www.europarl.europa.eu

From: [redacted]
Sent: 15 May 2019 17:29
To: [redacted]
Cc: [redacted] European Data Protection Supervisor <EDPS@edps.europa.eu>
Subject: Request for information | 2019-0373

Dear [redacted],

I hope this email finds you very well. I'm writing you regarding the informal consultation on the European Parliament's 'efficient printing' system (EDPS case file 2019-0373).
We thank you for the additional information you provided by email on 17/04/2019.
After the analysis of the documentation sent, we kindly ask you to clarify the following four points:

1. **Anonymous data**
   The personal data processing record states on page 3 that '[a]nonymised data will be used for statistical purposes in order to have a better overview of the paper and toner consumption'. Could you please provide additional details on what kind of anonymous data will you collect for statistical purposes and why you deem that such data should be considered anonymous. Is it, for example, 800 pages, toner consumption 50% on week 15?
2. **Complete diagram of the data flow**
   If available, could you please provide us with a complete diagram of the dataflow of the 'efficient printing' system.
3. **Data retention period**
   The personal data processing record states on page 5 that '[e]ncrypted records in databases (stored on the 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'. Could you please clarify the need for this data retention and what kind of personal data will be retained.
4. **Data encryption**
   You mention the type of encryption for the HDD data. Do you use the same encryption method (AES256-bit) for the other encrypted system?

We would appreciate if you could send us the information requested above by 11 June.
Thank you in advance for your collaboration.
Kind regards,

[redacted]
European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
@EU_EDPS www.edps.europa.eu

---

[1] The EDPS has issued a list of data processing subject to the DPIA obligation under Article 39(4) of the Regulation. Prima facie, it appears the 'efficient printing' system would not fall under this obligation. The list is available at: https://edps.europa.eu/data-protection/our-work/publications/guidelines/data-protection-impact-assessment-list_en.