EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
SUPERVISOR

[redacted]
Head of Unit - [redacted]

[redacted]
Head of Unit - [redacted]

European Parliament
60 rue Wiertz
B-1047 - Bruxelles

Brussels, 15 January 2021

WRW/[redacted]/[redacted]/[redacted]/ D(2021) [redacted] **C 2019-0971**
Please use edps@edps.europa.eu **for all correspondence**

Subject: EDPS Decision on the own initiative investigation on the personal data processing activities of the European Parliament's Wi-Fi network services (case 2019-0971)

Dear [redacted],
Dear [redacted],

Please find attached the European Data Protection Supervisor Decision of 15 January 2021 relating to the EDPS own initiative investigation on the European Parliament's personal data processing activities in the context of its Wi-Fi network services.

The EDPS wishes to thank you for your cooperation in the EDPS case 2019-0971.

Yours sincerely,

[e-signed]

Wojciech Rafał WIEWIÓROWSKI

cc: [redacted], Data Protection Officer of the European Parliament

EDPS Decision on own initiative investigation in the context of the European Parliament's personal data processing activities regarding the Wi-Fi network services

I. INTRODUCTION

This Decision sets out the EDPS's findings following its own-initiative investigation into the processing of personal data related to the European Parliament's (the 'Parliament's' or 'EP's') Wi-Fi services.

The EDPS issues this Decision based on Articles 57(1) (f) and 57(1)(g) of Regulation (EU) 2018/1725 (the 'Regulation')[1]. The focus of this Decision is on the compliance of the Parliament's activities with the provisions of the Regulation relating to the transparency of the processing, the information to be provided to data subjects and the technical and organisational measures relating to the security and confidentiality of the processing.

II. BACKGROUND

On 18 November 2019, the EDPS opened its own-initiative investigation, following a media report and consequent complaint cases regarding the collection of visitors' personal data by the European Parliament through its Wi-Fi network services.

During the investigation, the EDPS requested information on the types of personal data processed by the Parliament through its Wi-Fi services, the purpose of such processing, monitoring activities, data retention periods, recipients of the personal data collected and otherwise processed, transmissions and transfers of personal data and location of data storage, in the context of the Parliament's Wi-Fi services. Where necessary, the EDPS requested relevant documentation.

The information and documentation requested was transmitted to the EDPS via email correspondence. An on-site visit to the Parliament's premises was planned for March 2020, which was however cancelled due to the Covid-19 pandemic. In view of the continuation of the pandemic, and thus the infeasibility for an on-site visit, the EDPS requested further clarifications in a number of aspects in order to conclude the investigation.

III. FINDINGS, ORDER AND RECOMMENDATIONS

Activities taking place in the context of the Parliament's Wi-Fi networks must comply with the requirements of the Regulation, insofar as they concern processing of personal data. The EDPS investigation found a significant issue regarding the definition of personal data processing, which consequently had an impact on the transparency of the processing and the information to be provided to data subjects. The EDPS further identified additional issues, mainly technical, regarding, in particular, the technical and organisational measures relating to the security of processing as well as the security and confidentiality of transmissions and transfers of personal

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC; OJ L 295, 21.11.2018, p. 39–98. References to articles in this document refer to the Regulation.

data in the context of investigations. The EDPS suggests improving the second category of identified issues by means of recommendations.

1. Processing of personal data for the use of EP-Private and EP-Visitors Wi-Fi services and information to be provided to the data subjects

The Parliament's letter of 7 September 2020 states that information such as IP addresses and network device identifiers are considered technical data, which are used to route network messages to the correct devices.

Article 3(1) of the Regulation defines personal data as any information relating to an identified or identifiable natural person. In this context, identifiable natural person refers to a person who can be identified, directly or indirectly, by reference, among others, to an identifier, such as name, identification number, an online identifier.

In order to determine whether a natural person is identifiable, all the means that could be used by the controller or any other person for the direct or indirect identification of the natural person should be taken into account. According to Recital 16 of the Regulation, objective factors, such as the costs relating to and the time required for the identification, as well as the available technology should be considered in order to ascertain whether any such means for identification are likely to be used.

According to Recital 18 of the Regulation, natural persons may be associated with online identifiers provided by their devices, applications and protocols, such as internet protocol addresses (IP addresses), cookie identifiers or other identifiers. These information can lead to the identification of the natural persons, in particular when combined with unique identifiers and other information received by the servers.

In practice, IP addresses are not recorded in isolation, but in combination with other attributes such as the MAC address, which can uniquely identify a device, the connection time and the access point to which the device is connected (geographical information). This combination provides additional possibilities for the identification of the individual, to which the record relates, either by the controller or by another entity that may obtain access to this record. European institutions should ensure that when they record IP addresses in conjunction with other attributes and device identifiers, the resulting records are treated as personal data.

Based on the above, the EDPS considers, in line with the Regulation, that records containing IP addresses in conjunction with other attributes and device identifiers constitute personal data,[2] contrary to the characterisation of such data by the Parliament. Therefore, their processing is covered by the Regulation.

This interpretation is also in line with the Article 29 Data Protection Working Party (WP29) Opinion 4/2007 on the concept of personal data, in which the status of IP addresses as personal

[2] Guidelines on the protection of personal data processed through web services provided by EU institutions, 7 November 2016. Available at https://edps.europa.eu/data-protection/our-work/publications/guidelines/web-services_en.

data was addressed.[3] This classification has also been the subject of cases at the Court of Justice of the European Union.[4]

The fact that the processing of IP addresses is covered by the Regulation, entails that the data protection principles, as laid out in the Regulation, should be respected, and appropriate security and organisational measures should be put in place to ensure processing of the IP addresses in a manner compliant with the Regulation. The obligation to ensure compliance with the Regulation in this respect lies with the controller.[5] The Parliament, as the controller of the processing operations at hand, failed to comply with the Regulation, as a consequence of its interpretation of the scope of the concept of personal data.

In light of the above, the EDPS considers that the processing of personal data for the use of EP-Private and EP-Visitors Wi-Fi services, as defined by the Parliament, insofar as the processing of IP addresses is concerned, is not in line with Article 3(1) of the Regulation and does not comply with the principle of transparency (Articles 4(1) and 14 of the Regulation) and the data subject's right to information (Articles 15 and 16 of the Regulation).

The EDPS, therefore, orders the Parliament, pursuant to Article 58(2)(e) of the Regulation, to update the 'Wi-Fi Terms and Conditions of use for EP-Private' and 'Wi-Fi Terms and Conditions of use for EP-Visitors' documents in order to reflect information relating to the processing of personal data, in accordance with Articles 14, 15 and 16 of the Regulation.

Furthermore, in relation to the identified issue, the EDPS issues the following **recommendation** to the Parliament:

1. Review already existing policies, outside the context of the EP-Private Wi-Fi, and ensure that when collecting or otherwise processing IP addresses in conjunction with other attributes and device identifiers, these are treated and protected as personal data, in accordance with the Regulation.

2. Enhanced transparency

In its letter of 11 December 2019, the Parliament explains that information on the data protection aspects relating to the European Parliament Service Desk (EPSD) ticketing system, which is the Parliament's user support application, to the EP ICT supervision infrastructure and network data capture, in the context of which falls the provision and supervision of the EP-Private and EP-Visitors Wi-Fi networks, as well as of those relating to the investigations are available online at the Parliament's Data Protection Registry, through the respective records of processing activities, in line with Article 31 of the Regulation. The records concerned are No 156, 177 and 392, respectively.

These records include a section with information on how data subjects can exercise their rights to access, rectification, objection and data portability. In particular, the record of the EPSD ticketing system states that in case data subjects wish to exercise their abovementioned data

[3] WP29 Opinion 4/2007 on the concept of personal data, 20 June 2007. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.
[4] Case C-70/10 Scarlet Extended SA: "Those addresses are protected personal data because they allow those users to be precisely identified" (paragraph 51); Case C-582/14 Breyer: "Article 2(a) of Directive 95/46 must be interpreted as meaning that a dynamic IP address registered by an online media services … constitutes personal data … where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person" (paragraph 49).
[5] See Article 4(2) of Regulation (EU) 2018/1725.

protection rights, they should contact the helpdesk. No functional email is provided, nor a link to an online data protection notice. The records of processing activities relating to the investigations and to the EP ICT infrastructure and network data capture provide a functional email address through which data subjects can request exercise of their data protection rights, however they provide no link to an online data protection notice.

Article 4(1)(a) of the Regulation establishes the principles of lawfulness, fairness and transparency that apply to all personal data processing operations. Article 14 of the Regulation imposes the obligation on the controller to provide data subjects with information regarding the processing of their personal data in a transparent and easily accessible form. This information should be presented in a clear and plain language before the processing starts. The Regulation's transparency and information requirements should be met through a specific data protection notice. The information included in the data protection notice should be in line with Articles 15 and 16 of the Regulation.

Although the data protection notice is not strictly speaking part of the record, linking the two increases transparency.[6]

Recommendations:

2. Update all three records of the concerned processing activities in order to include links to the relevant online data protection statements, so that transparency is enhanced.
3. Compare the information between the records and the data protection notices and align the text, where necessary. This recommendation is linked to the order issued under Article 58(2)(e) of the Regulation in section III.1 of this Decision.

3. Risk assessment based on Article 33 of the Regulation

The Parliament has conducted two high-risk pre-assessments on its Wi-Fi services, one on the 'IT Service Support Management System' and one on the 'EP ICT Supervision Infrastructure and Network Data Capture'. This threshold assessment was done in view of assessing whether a Data Protection Impact Assessment (DPIA) under Article 39 of the Regulation should be conducted. The conclusion of this assessment was that no DPIA was required.

The EDPS submits that this was not enough: apart from the abovementioned threshold assessment, the Parliament should in addition assess data security risks, following Articles 26 and 33 of the Regulation: the controller should ensure that appropriate technical and organisational measures are in place so that the security and confidentiality of the processing are guaranteed. In order to do so, there should be an evaluation of the risks inherent to the processing and, subsequently, an implementation of measures to mitigate those risks.

The Parliament has informed the EDPS its plans to conduct a risk assessment in the context of its Wi-Fi infrastructure renewal project. Based on the above, the Parliament's Risk assessment should also include Article 33 of the Regulation as well as the EDPS Guidance on security measures for personal data processing,[7] which can provide essential support for this exercise.

[6] Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies. Part I: Records and threshold assessment, 16 July 2019. Available at: https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf

[7] Guidance on Security Measures for Personal Data Processing - Article 22 of Regulation 45/2001, 21 March 2016. Available at https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en .

Recommendations:

4. The Parliament, with the involvement of the EP Data Protection Officer (DPO), should perform a security risk assessment of the two systems, the Wi-Fi system and the EP Service Desk system, in accordance with Article 33 of the Regulation, paying particular attention to the 'risks of varying likelihood and severity for the rights and freedoms of natural persons'. The Parliament should ensure that this Risk Assessment is regularly reviewed in order to address developments in security requirements.
5. In the context of the aforementioned Risk Assessment, as regards retention periods of the two systems, the Parliament should improve the justification for the chosen time periods, in order to find the balance between the need to keep log files for a certain time and the risks for the rights and freedoms of individuals whose the personal data are processed by the two systems.
6. The Risk Assessment should also assess any data transfers to other internal or external entities as well as the possible data correlations between the two systems.
7. The Parliament should consult the EP DPO on all these matters.

During the investigation, it became apparent that log files, both 'live' logs, retained for 30 days and zipped logs, retained for six months, contain the following personal data: device mac addresses, usernames that have different types of values and occasionally contain names of natural persons, locations of the Wi-Fi access points and distinction between 'MEP' and 'not MEP'.

Recommendation:

8. The Parliament should justify why these attributes and device identifiers are recorded in the context of the aforementioned Risk Assessment.
9. The Parliament should additionally consider the possibility of 'pseudonymisation and encryption of personal data', in line with Article 33 of the Regulation, in order to minimise the risk for the rights and freedoms of the users, as well to comply with the principle of data minimisation in the context of the personal data processed by the two systems. For example, the EPSD system should retain the absolute minimum necessary personal data, while the Wi-Fi system should only record pseudonymised identifiers within 'live' and/or zipped logs. In this context, the Parliament should consult its DPO on the implementation of relevant Privacy Enhancing Technologies.

4. Security and confidentiality of transmissions and transfers of personal data in the context of investigations

The Parliament's letter of 7 September 2020 describes the procedure for the transfers[8] and transmissions of data, including personal data, to other authorities, such as OLAF or law enforcement authorities, or services of the Parliament in charge of conducting investigations. According to the described procedure, the requested data are transferred and/or transmitted in paper form or on a mobile storage media, such as USB stick or external hard drive, depending on the volume of the data concerned. Transfers and transmissions are made from one hand to another, either by the officers in charge or through an intermediary person, acting upon the Parliament's instructions, with a 'chain of custody' document, which every person involved in the transfer or transmission signs.

In accordance with Article 33(1) and (2) of the Regulation, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to

[8] The information and recommendations under this section are without prejudice to the conditions for transfers of personal data to third countries and international organisations (Articles 46 to 51 of the Regulation).

the risks presented by the processing. Such risks include accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data stored or otherwise processed. Given the fact that information processed for administrative inquiries and investigation purposes usually includes a significant amount of personal, including special, data[9], particular emphasis should be given on the safeguarding of these data.

Transferring or transmitting (special) personal data in paper files, increases the risk of unauthorised access to these files (and to the personal data contained therein) by personnel who would otherwise not have access to them or even by third parties, in case of loss of the paper files. Similarly, storage and otherwise processing of personal data on and through removable storage media might provide a higher level of protection for the personal data, only in cases where the files contained therein are properly encrypted.

Based on the above, the Parliament should implement appropriate technical and organisational measures to ensure security, including confidentiality, of the processing of personal data within the context of administrative inquiries or other internal and external investigations, in accordance with Article 33 of the Regulation.

Recommendations:

10. Review existing transmissions and transfers policies, regarding administrative enquiries or other internal and external investigations, in view of abolishing such processing of personal data in paper form.
11. When using removable storage media to transfer documents including personal data ensure that the documents are protected by encryption with the following requirements: (i) AES 256 encryption standard - or equivalent, (ii) the encryption password has sufficient complexity so it cannot be guessed by a malicious person[10], (iii) the encryption password is kept separately from the encrypted files and (iv) the encryption password is sent to the intended recipient using a different channel than the one used for the transport of the encrypted file (e.g. by voice call, instant message).
12. Consider establishing a secure emailing system for secure personal data transmission, that is able to ensure (i) the authenticity of the sender, so that the recipient can have the assurance that the message was sent by a legitimate sender (ii) the confidentiality of the transmitted information so that only the intended recipient is able to access it and (iii) the integrity of the transmitted information so that the receiver can verify if the information was tampered with during the transmission.
13. Update the chain of custody template, so that it includes a specific reference to Regulation (EU) 2018/1725. Put additional organisational measures in place, such as making mandatory the signature of confidentiality declarations by the officers involved in the transmission and/ or transfers procedure,[11] in order to ensure confidentiality of the processing by the Parliament's personnel and externals involved, while promoting a data protection culture among the persons involved. Ensure that the EP DPO is involved and consulted in cases where there is ambiguity on the amount of personal data that needs to be transmitted and/ or transferred.

[9] Guidelines on processing personal information in administrative inquiries and disciplinary proceedings, 18 November 2016. Available at https://edps.europa.eu/sites/edp/files/publication/16-11-18_guidelines_administrative_inquiries_en.pdf.
[10] Use complex passwords longer than eight (8) characters, which contain alphanumeric and special characters.
[11] Guidelines on processing personal information in administrative inquiries and disciplinary proceedings, 18 November 2016. Available at https://edps.europa.eu/sites/edp/files/publication/16-11-18_guidelines_administrative_inquiries_en.pdf.

14. Set up periodic reviews of the existing transmissions and transfers procedure, with the view of updating parts that are obsolete, also in light of the latest technological developments relating to the security of the processing.

Finally, the EDPS invites the European Parliament to inform of the outcome of any current ongoing projects, developments and/ or initiatives relating to the Parliament's Wi-Fi network services and periodically update the EDPS on the measures taken in the context of improving compliance with EDPS guidance documents and the Regulation.

IV. CONCLUSION

On the basis of the facts and findings as described above, the EDPS decides to:

a) order the Parliament, pursuant to Article 58(2)(e) of the Regulation, to update the 'Wi-Fi Terms and Conditions of use for EP-Private' and 'Wi-Fi Terms and Conditions of use for EP-Visitors' documents in order to reflect information relating to the processing of personal data, in accordance with Articles 14, 15 and 16 of the Regulation. The Parliament should address this order within three (3) months since the date of this Decision;
b) issue the abovementioned recommendations to the European Parliament; and
c) close its own initiative investigation on the processing of personal data within the context of the European Parliament's Wi-Fi network services, without prejudice to any new evidence that may affect this Decision.

Pursuant to Article 64(1) of the Regulation, any action against a decision of the EDPS shall be brought before the Court of Justice of the European Union within two months from the adoption of the present Decision and according to the conditions laid down in Article 263 TFEU.

The EDPS intends to make public the fact of our investigation and the outcome, including the actions taken in response by the European Parliament.

Brussels, 15 January 2021

[e-signed]

Wojciech Rafał WIEWIÓROWSKI