



Decision of the European Data Protection Supervisor in complaint case 2019-0086 submitted against the European Parliament

The EDPS,

Having regard to Article 16 TFEU, Article 8 of the Charter of Fundamental Rights of the EU, and Regulation (EU) 2018/1725¹ (the Regulation), in particular its Article 57(1)(e),

Issues the following Decision:

PART I - Proceedings

On 25 January 2019, the Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI, federal German data protection authority) referred (with the complainant's agreement) a complaint to the EDPS because it referred to processing of personal data by an EU institution (the European Parliament).

On 29 January 2019, the EDPS acknowledged receipt to the complainant and the BfDI. In this message, the EDPS noted that since knowing the complainant's identity was not necessary for the European Parliament (EP) to react to the allegations, it would not disclose the complainant's identity to the EP.

On the same day, the EDPS informed the EP about the complaint, providing a summary of the allegations made and requesting the EP's position on these, as well as and requesting some clarifications.

On 15 February 2019, the EP answered, providing its position and most of the clarifications requested.

On 21 February 2019, the EDPS requested some additional clarifications.

On 12 April 2019, the EDPS informed the complainant about the progress of his file.

Following several reminders, the EP provided the remaining clarifications on 29 April 2019.

PART II - The Facts

Allegations of the complainant

The complainant raised an issue about the visitor registration tool / visitors' meeting point available here: <http://www.europarl.europa.eu/fivisit/>.

This tool serves to register visitors who come as part of groups; a contact point for the group enters the personal data of the other group members for registration.

According to the complainant, the tool has a functionality to "check if the email address is already in the system", allowing to retrieve the information associated to already registered e-mail addresses (first and family name, gender, date of birth, nationality, full address, occupation, special needs / disability, telephone number, languages). According to the complainant, there is no limit for checking e-mail addresses, so a user could systematically try

¹ OJ L 295, 21.11.2018, p. 39–98.

a large number of addresses to retrieve personal data of persons who are not part of the visitors group they are registering.

Based on the complainant's description of the facts, any user could retrieve this information for any email address registered in the system.

Comments of the data controller

The EP confirmed that it was indeed possible for users to check whether an e-mail address was already registered and that the system returned the items mentioned by the complainant.

The EP stressed that this search was only possible with the e-mail address and not with any other field, such as the name. According to the EP, in many cases, contact data is only retained in this part of the system for approximately one month after the visit, and therefore the look-up functionality will only return information for individuals who were part of a visitors group during that time.

The EP noted that its IT department was working on removing the functionality. The EP also informed that it was in the final testing phase for a new IT system for visitor registration, replacing the current system. A look-up as described by the complainant would not be possible in the new system.

PART III - Legal Analysis

Admissibility of the complaint

The processing is carried out by the EP using automated means and thus falls within the scope of the Regulation (Article 2(1) and (5) of the Regulation). The complainant is a contact point for a visitor group (and presumably a visitor, too). Thus, the complainant's personal data were potentially also affected by the alleged violation of the Regulation. The complaint is admissible under Article 63 of the Regulation.

Alleged violation of Article 4(1)(b)

The complainant did not mention which specific provision of the Regulation the EP violated in their view. This complaint is about personal data that are potentially made available, although their availability is not necessary in the light of the purpose pursued. The complaint therefore concerns an alleged breach of the data minimisation principle in Article 4(1)(b) of the Regulation:

“Personal data shall be [...] adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)”

The data minimisation principle states that both the amount of personal data collected and the extent of their processing have to be limited to what is necessary for the defined legitimate purposes of the processing operations to be fulfilled.

The EP has not provided any justification for this lookup functionality and none is obvious.

Additionally, this lookup functionality could indeed create risks to data subjects: It can be exploited to obtain personal data of visitors from organisations with known naming conventions for their e-mail addresses (e.g. universities or large companies), which may be further processed without a lawful basis or even abused.

Therefore, the existence of this functionality is a **breach of the data minimisation principle in Article 4(1)(b) of the Regulation**.

The EDPS also takes note that the EP is in the process of developing a new system for visitor registration that will not contain such a functionality. For the development of the new system, the EP should ensure that as a whole, it will be in line with the principle of data protection by design and by default (Article 27 of the Regulation).

PART IV - Conclusion

As established in the legal analysis above, there has been a breach of Article 4(1)(b) of the Regulation.

Therefore, the EDPS **reprimands the European Parliament, under Article 58(2)(b) of the Regulation, for this breach.**

The EDPS also **orders the European Parliament, under Article 58(2)(e) of the Regulation, to bring the contested processing operations in line with the Regulation by removing the lookup functionality from the current system within one month from the date of this Decision, should it still be in use.**

Furthermore, the EDPS wishes to be kept informed of further developments regarding the new IT system for visitor registration, replacing the current system.

Done at Brussels, [insert date]

[signed]