Decision of the European Data Protection Supervisor in complaint case [redacted] submitted by [redacted] against [redacted]

The EDPS,

Having regard to Article 16 TFEU, Article 8 of the Charter of Fundamental Rights of the EU, and Regulation (EC) 45/2001,[1]

Has issued the following decision:

PART I
Proceedings

On 7 April 2019, the EDPS received a complaint under Article 33 of Regulation (EC) 45/2001 (the Regulation) from [redacted] (the complainant) against [redacted] – Case [redacted]

The EDPS repeatedly invited the complainant to fill in the online complaints form to better structure the complaint, but she decided not to do so.[2]

The EDPS requested written comments from the controller on the complainant's allegations on 21 January 2020. The controller replied on 2 March 2020.

The complainant was asked to comment on the controller's reply, but has not provided any comments to the EDPS within the set deadline.

PART II
The facts

1. Allegations of the complainant

The complainant alleges that on 24 October 2018, she requested from [redacted] a '... list of documents, a copy of them and a list of all accesses to [her] personal information, with the indication of the personal information to which access was given and the individuals that had access to [her] data, as well as the reason justifying it'.

The complainant added that she has not yet been given access to her requested personal data.

[1] OJ L 8 of 12.01.2001. In the meantime, the new Regulation has entered into force: 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) 45/2001 and Decision No 1247/2002/EC, OJ L 295 of 21.11.2018. Nevertheless, case 2019-0374 was examined in the light of Regulation (EC) 45/2001, which was applicable when the facts occurred.

[2] The complainant was slow to react on these invitations and the EDPS therefore also asked her whether she wanted to pursue her complaint, which she confirmed.

In addition, the complainant also expressed concerns that some sensitive information was sent to her via email, which she does not consider a safe means of communication.

2. Comments of the data controller

In their reply, the controller stated that the complainant's allegations were incorrect, since they had given the complainant access to her personal data.

In particular, the controller explained that:

'- On 30 January 2019, DPO informed the complainant on all aspects of her request and in particular on the different Human Resources (HR) fields where [redacted] was processing her personal data (...). In later emails of 12/02/2019, the DPO completed the information related to information and Communication Technologies Unit (ICT) and Corporate Service Unit (CSU) respectively.

- On 5/04/2019 the complainant received her personal data from the CSU. The HR Unit sent her the personal data previously announced in the above email of 30 January 2019, with emails dated from 11/04/2019, and 13/06/2019 (2 emails that same day).

On 7 April 2019, the DPO (...):
- summarised the situation regarding the personal data she had received (from CSU) and the possibility she had been given to receive her medical data directly from the [redacted] Medical Service. The Medical Service had sent the complainant all her personal medical data back in 2014 and was no longer in the possession of any further medical data related to her (...).
- confirmed that no ICT related data were available anymore, as they had been deleted after she left and according to the retention period.
- regarding the HR personal data, the DPO explained the categories of data she had already received and announced that further personal data will be sent to her directly from the responsible HR Unit.'

The controller added that '[o]n 11 April 2019, the DPO had also replied to her alleged "breach of security", and explained the technical security measures [redacted] used to provide her with personal data in a secure and confidential way (...). Furthermore, the complainant did not react to the DPO's question to know whether she was still willing to receive the missing personal data processed by [redacted] (...) Therefore and complying with the data protection access requirements, the HR Unit, in its two e-mails of 13/06/2019 sent her the remaining personal data in an encrypted form and password protected'.

PART III
Legal analysis

1. Admissibility of the complaint

The complainant is a former staff member of an EU institution. As such, she may lodge a complaint under Article 33 of the Regulation alleging a breach of the provisions of the Regulation. The complaint is therefore admissible.

2. Alleged violation of Article 13 of the Regulation - right of access by the data subject

The right of access to personal data under Article 13 of the Regulation stipulates that data subjects shall have the right to obtain without constraint from the controller and within three months, communication in an intelligible form of the data undergoing processing and any available information as to their source.

Furthermore, Article 26a of the Staff Regulations provides that staff members have the right to acquaint themselves with their medical files, in accordance with arrangements laid down by the institutions.

On 24 October 2018, the complainant requested [redacted] to have access to her personal data, including to her medical file, processed by them.

[redacted] has provided the complainant with access to her personal data in several instances via the DPO and the HR Unit, as proven by the emails sent on 31 October 2018, 19 and 26 November 2018, 30 January 2019, 12 and 26 February 2019, 2 and 7 April 2019, and 13 June 2019.[3]

However, [redacted] sent the last email to the complainant with her personal data almost eight months after the initial request, thus exceeding the initial three months deadline.

The EDPS considers that [redacted] promptly replied in part to the complainant's access request, but that the delay in providing full access exceeded by almost five months the legal deadline stated in Article 13 of the Regulation. Even when taking into account the complexity of the request, involving the coordination of several [redacted] units, the EDPS believes that the final reply to the complainant should not have been sent almost five months after the established three-month deadline[4]. The controller should at least have informed the complainant regularly of any potential delay in complying with her request.

The EDPS takes note of the fact that the controller repeatedly requested clarifications from the complainant on her access request and that complainant showed a certain lack of cooperation. She therefore contributed to the delay. However, the complainant's request dated 24 October 2018, and the subsequent interaction with the DPO, show that the controller had the necessary elements to handle the complainant's access request to her personal data in a more timely manner.

In light of the above, the EDPS considers that the complainant has not been given timely access to her personal data in accordance with Article 13 of the Regulation, since the last personal data were sent to her more than three months after her initial request.

[3] Moreover, the complainant had already requested to have access to her personal data in 2014 and [redacted] had provided her with access to her personal data, including health data (according to a letter dated of 27 January 2014).

[4] As a term of reference, Article 14(3) of Regulation (EU) 2018/1725 establishes three months as a maximum deadline to provide the right of access, one month being the standard. As stated above this regulation is not applicable in this case, but it illustrates the short deadlines envisaged by the legislator in both legal documents regarding the provision of rights to data subjects.

3. Alleged violation of Article 22 of the Regulation - security of the data processing

Article 22 of the Regulation regarding the security of the personal data processing, states that, having regard to the state of the art and the cost of their implementation, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.

The EDPS notes that the HR Unit sent emails to the complainant on 13 June 2019 in a zip file protected by password. The password was then sent via text message. Based on the available information, this seems to be appropriate given the requirements of Article 22 of the Regulation.

The EDPS also notes that the complainant made at least some of her access requests by email and could therefore reasonably expect to receive a reply by the same means of communication. Furthermore, she never explicitly requested to receive the information by other means, such as by postal mail.

However, [redacted] should ensure that they comply with the requirements of security laid down in Article 33 of Regulation (EU) 2018/1725[5] when providing access to data subjects.

PART IV
Conclusion

In light of the above, the EDPS concludes that there was a violation of Article 13 of the Regulation by the [redacted], since the complainant was not given timely access to her personal data within three months from the date of her initial request.

Therefore, the **EDPS admonishes [redacted] for this breach, under Article 47(1)(d) of the Regulation and orders [redacted] to implement measures within three months to ensure compliance with the deadlines set out in Article 14(3) of Regulation (EU) 2018/1725, under Article 58(2)(e) of this Regulation**.

Regarding the alleged violation of Article 22 of the Regulation, the EDPS found no breach, since the complainant's personal data were transmitted to her with appropriate security measures.

Having into consideration all the above, the EDPS has decided to close the present case.

Done at Brussels, 3rd June 2020

[**signed**]

Wojciech Rafał WIEWIÓROWSKI

[5] Provision replacing Article 22 of Regulation (EC) 45/2001.