PRESS RELEASE

EDPS/2024/05
Brussels, 11 March 2024

European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies

Following its investigation, the EDPS has found that the European Commission (Commission) has infringed several key data protection rules when using Microsoft 365. In its decision, the EDPS imposes corrective measures on the Commission.

The EDPS has found that the Commission **has infringed several provisions of Regulation (EU) 2018/1725**, the EU's data protection law for EU institutions, bodies, offices and agencies (EUIs), including those **on transfers of personal data outside the EU/European Economic Area (EEA)**. In particular, the Commission has failed to provide appropriate safeguards to ensure that personal data transferred outside the EU/EEA are afforded an essentially equivalent level of protection as guaranteed in the EU/EEA. Furthermore, in its contract with Microsoft, **the Commission did not sufficiently specify what types of personal data are to be collected and for which explicit and specified purposes when using Microsoft 365**. The **Commission's infringements as data controller also relate to data processing**, including transfers of personal data, carried out **on its behalf**.

Wojciech Wiewiórowski, EDPS, said: *"It is the responsibility of the EU institutions, bodies, offices and agencies (EUIs) to ensure that any processing of personal data outside and inside the EU/EEA, including in the context of cloud-based services, is accompanied by robust data protection safeguards and measures. This is imperative to ensure that individuals' information is protected, as required by Regulation (EU) 2018/1725, whenever their data is processed by, or on behalf of, an EUI."*

The EDPS has therefore decided to order the Commission, effective on **9 December 2024**, to **suspend all data flows** resulting from its use of Microsoft 365 **to Microsoft** and to its affiliates and sub-processors **located in countries outside the EU/EEA not covered by an adequacy decision**. The EDPS has also decided to order the Commission to **bring the processing operations** resulting from its use of Microsoft 365 **into compliance with Regulation (EU) 2018/1725. The Commission must demonstrate compliance with both orders by 9 December 2024**.

The EDPS considers that **the corrective measures it imposes (see annex for a detailed excerpt) are appropriate, necessary** and **proportionate in light of the seriousness and duration of the infringements found.**

Many of the infringements found concern all processing operations carried out by the Commission, or on its behalf, when using Microsoft 365, and impact a large number of individuals.

The EDPS also takes into account the need **not to compromise the Commission's ability to carry out its tasks in the public interest or to exercise official authority vested in the Commission, and the need to allow appropriate time for the Commission to implement the foreseen suspension of relevant data flows, and to bring the processing of data into compliance with Regulation (EU) 2018/1725.**

The measures imposed by the EDPS in its decision of 8 March 2024 are without prejudice to any other or further action that the EDPS may undertake.

The findings of infringements and corrective measures imposed by the EDPS in its decision can be found in annex.

Background information

The rules for data protection in the EU institutions, bodies, offices and agencies, as well as the duties of the European Data Protection Supervisor (EDPS), are set out in **Regulation (EU) 2018/1725**.

Wojciech Wiewiórowski (EDPS) was appointed by a joint decision of the European Parliament and the Council to serve a five-year term, beginning on 6 December 2019.

About the EDPS' investigation into the Commission's use of Microsoft 365: This investigation was opened in May 2021 following the *Schrems II* judgment. Its aim was to verify the Commission's compliance with the Recommendations previously issued by the EDPS on the use of Microsoft's products and services by EU institutions and bodies. This investigation is part of the EDPS' actions in the context of the EDPS' participation in the 2022 Coordinated Enforcement Action of the EDPB. For more information, please read the EDPB Report on the 2022 Coordinated Enforcement Action.

About EDPS Investigations: For more information on the EDPS' investigation process, please find the EDPS Investigation Policy, EDPS Investigation Factsheet, on the EDPS Website.

The European Data Protection Supervisor (EDPS) is the independent supervisory authority for the protection of personal data and privacy and promoting good practice in the EU institutions and bodies.

He does so by:

- monitoring the EU administration's processing of personal data;
- monitoring and advising technological developments on policies and legislation that affect privacy and personal data protection;
- carrying out investigations, including in the form of data protection audits/inspections;
- cooperating with other supervisory authorities to ensure consistency in the protection of personal

EDPS - The EU's Independent Data Protection Authority

Questions can be directed to press@edps.europa.eu.

edps.europa.eu

Annex: list of corrective measures and infringements following the EDPS investigation into the use of Microsoft 365 by the European Commission

Corrective measures

1. The EDPS has decided to take the following corrective measures in respect of the infringements detailed below:

   1.1. to order the Commission, under Article 58(2)(j) of Regulation (EU) 2018/1725 and with effect from 9 December 2024, to suspend all data flows resulting from its use of Microsoft 365 to Microsoft and to its affiliates and sub-processors, located in third countries not covered by an adequacy decision as referred to in Article 47(1) of the Regulation, and to demonstrate the effective implementation of such suspension (*infringements set out in paragraphs 3.a and b, first indent, and 4 below*);

   1.2. to order the Commission, under Article 58(2)(e) of Regulation (EU) 2018/1725, to bring the processing operations resulting from its use of Microsoft 365 into compliance, and to demonstrate such compliance, by 9 December 2024, by:

      1.2.1. carrying out a transfer-mapping exercise identifying what personal data are transferred to which recipients in which third countries, for which purposes and subject to which safeguards, including an onward transfers (*infringements listed in paragraph 3.a and b, first indent, below*);

      1.2.2. ensuring that all transfers to third countries take place solely to allow tasks within the competence of the controller to be carried out *(infringement listed in paragraph 3.d below*);

      1.2.3. ensuring, by way of contractual provisions concluded pursuant to Article 29(3) of Regulation (EU) 2018/1725 and of other organisational and technical measures, that:

         a) all personal data are collected for explicit and specified purposes (*infringements listed in paragraph 2.a and b below)*;

         b) the types of personal data are sufficiently determined in relation to the purposes for which they are processed (*infringements listed in paragraph 2.a and b below)*;

         c) any processing by Microsoft or its affiliates or sub-processors is only carried out on the Commission's documented instructions, unless, for processing within the EEA, required by EU or Member State law, or, for processing outside of the EEA, third-country law that ensures a level of protection essentially equivalent to that in the EEA, to which Microsoft or its sub-processors are subject (*infringements listed in paragraphs 2.b and c, 3.a and 4 below)*;

         d) no personal data are further processed in a manner that is not compatible with the purposes for which the data are collected, in accordance with the criteria laid down in Article 6 of Regulation (EU) 2018/1725 (*infringement listed in paragraph 2.d below)*;

         e) any transmissions to Microsoft Ireland or its affiliates and sub-processors located in the EEA comply with Article 9 of Regulation (EU) 2018/1725 (*infringement listed in paragraph 2.e below*);

         f) for personal data processed in the EEA, only EU or Member State law prohibits notification to the Commission of a request for disclosure, and, for personal data processed outside the EEA, any prohibition of such notification constitutes a necessary and proportionate measure in a democratic society respecting the essence of the fundamental rights and freedoms recognised by the Charter, as required by Article 29(3)(a) of Regulation (EU) 2018/1725, in particular as

interpreted in light of the *Schrems II* judgment (*infringement listed in paragraph 4.a below*);

g) no disclosures of personal data by Microsoft or its sub-processors take place, unless, for personal data processed within the EEA, the disclosure is required by EU or Member State law, or, for personal data processed outside of the EEA, the disclosure is required by third-country law that ensures a level of protection essentially equivalent to that in the EEA, to which Microsoft or its sub-processors are subject (*infringements listed in paragraph 4.b below*).

1.3. to issue a reprimand to the Commission under Article 58(2)(b) of Regulation (EU) 2018/1725 (*all infringements listed below*).

Purpose limitation

2. The EDPS finds that the Commission, on 12 May 2021 ("the reference date") and continuously thereafter until 8 March 2024 ("the date of issuing EDPS' decision"):

a) has infringed Article 4(1)(b) of Regulation (EU) 2018/1725 by failing to:

- sufficiently determine the types of personal data collected under the 2021 Inter-institutional licencing agreement concluded with Microsoft Ireland ("2021 ILA") in relation to each of the purposes of the processing so as to allow those purposes to be specified and explicit;
- ensure that the purposes for which Microsoft is permitted to collect personal data under the 2021 ILA are specified and explicit;

b) has infringed Article 29(3)(a) of Regulation (EU) 2018/1725 by insufficiently determining in the 2021 ILA which types of personal data are to be processed for which purposes and by failing to provide sufficiently clear documented instructions for the processing;

c) has infringed Articles 4(2) and 26(1) in conjunction with Article 30 of Regulation (EU) 2018/1725 by failing to ensure that Microsoft processes personal data to provide its services only on documented instructions from the Commission;

d) has infringed Article 6 of Regulation (EU) 2018/1725 by failing to assess whether the purposes for further processing are compatible with the purposes for which the personal data have initially been collected;

e) has infringed Article 9 of Regulation (EU) 2018/1725 by failing to assess whether it is necessary and proportionate to transmit the personal data to Microsoft Ireland and its sub-processors (including affiliates) located in the EEA for a specific purpose in the public interest.

Transfers of personal data outside the EU/EEA

3. The EDPS finds that the Commission, on the reference date and, except with regard to point b), second indent, and to point c), continuously thereafter until the date of issuing the EDPS' decision:

a) has infringed Article 29(3)(a) of Regulation (EU) 2018/1725 by failing to clearly provide in the 2021 ILA what types of personal data can be transferred to which recipients in which third country and for which purposes, and to give Microsoft documented instructions in that regard;

b) has infringed Articles 4(2), 46 and 48 of Regulation (EU) 2018/1725 by failing to provide appropriate safeguards ensuring that data transferred enjoy an essentially equivalent level of protection to that in the EEA since it:

- has not appraised, either prior to the initiation of the transfers or subsequently, what personal data will be transferred to which recipients in which third countries and for which purposes, thereby not obtaining the minimum information necessary to determine whether any supplementary measures are required to ensure the essentially equivalent

level of protection and whether any effective supplementary measures exist and could be implemented;

- had not implemented effective supplementary measures for transfers to the United States taking place prior to the entry into force of the US adequacy decision, in light of the *Schrems II* judgment, nor has it demonstrated that such measures existed;

c) has infringed Articles 4(2), 46 and 48(1) and (3)(a) of Regulation (EU) 2018/1725 by:

- concluding the Standard contractual clauses ("SCCs") for transfers from the Commission to Microsoft Corporation without having clearly mapped the proposed transfers, concluded a transfer impact assessment and included appropriate safeguards in those SCCs;

- failing to obtain authorisation of those SCCs for transfers from the Commission to Microsoft Corporation from the EDPS pursuant to Article 48(3)(a) of Regulation (EU) 2018/1725;

d) has infringed Article 47(1) of Regulation (EU) 2018/1725 read in the light of Articles 4, 5, 6, 9 and 46 by failing to ensure that transfers take place "*solely to allow tasks within the competence of the controller to be carried out.*"

Unauthorised disclosures of personal data

4. The EDPS finds that the Commission, on the reference date and continuously thereafter until the date of issuing EDPS' decision:

a) has infringed Article 29(3)(a) of the Regulation, in particular as interpreted in the light of the *Schrems II* judgment, by not ensuring that, for personal data processed in the EEA, only EU or Member State law prohibits notification to the Commission of a request for disclosure, and that, for personal data processed outside the EEA, any prohibition of such notification constitutes a necessary and proportionate measure in a democratic society respecting the essence of the fundamental rights and freedoms recognised by the Charter;

b) has infringed Articles 4(1)(f), 33(1) and (2) and 36 of Regulation (EU) 2018/1725, by:

- not having assessed the legislation of all third countries to which personal data are envisaged to be transferred under the 2021 ILA and thereby failing to ensure that Microsoft and its sub-processors do not make disclosures of personal data within and outside of the EEA that are not authorised under EU law;

- failing to implement effective technical and organisational measures that would ensure processing in accordance with the principle of integrity and confidentiality within the EEA and, as part of an essential equivalence of the level of protection, also outside of the EEA.