# Cloud GDPR risks highlighted by European Commission ruling over Microsoft 365 use

**Client Alert** | 5 min read | 08.12.25

On 11 July 2025, the European Data Protection Supervisor, ("**EDPS**"), the independent supervisory authority, which oversees the processing of personal data by EU institutions, bodies, offices and agencies, ("**EUIs**") confirmed that the European Commission, ("**Commission**") has succeeded in bringing its use of Microsoft 365 within the requirements of applicable European data protection rules thanks to additional measures adopted by both the Commission and Microsoft.

## Background

Highlighting that no-one is above the law when it comes to data protection compliance, in May 2021 the Commission found itself the subject of an investigation by the EDPS, which decided to evaluate the Commission's use of Microsoft 365. The EDPS issued a Decision in respect of this investigation on 8 March 2024, ("**Decision**") which concluded that the Commission had infringed various provisions of Regulation (EU) 2018/1725 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, ("**Regulation**"), which essentially sets out the GDPR-like requirements that apply to EUIs.

The Commission's alleged violations related, variously, to purpose limitation, international personal data transfers and unauthorised personal data disclosures and the EDPS brought various corrective measures to bear on the Commission. During the recent enforcement proceedings, the EDPS considered the steps taken by the Commission in response to the EDPS's Decision and decided that the various breaches identified have now been rectified.

## Infringements

Regarding purpose limitation, the EDPS found that the Commission had contravened various rules. Among other things, the Commission's failure to ensure that Microsoft processed personal data to provide its services only on documented instructions from the Commission. Another issue was the failure to assess whether the purposes for further processing were compatible with the purposes for which the personal data were initially collected.

In respect of international personal data transfers, the EDPS found that the Commission failed in various ways to provide appropriate safeguards ensuring that transferred personal data enjoy an essentially equivalent level of protection to that in the European Economic Area, ("**EEA**"). For example, the Commission was held not to have appraised what personal data will be transferred, to which recipients, in which third countries and for which purposes, meaning that 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 been obtained.

Concerning unauthorised disclosures, the EDPS held that the Commission had failed 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 the EEA.

The EDPS decided to implement a number of corrective measures in relation to the various breaches of the rules. These included, for example, ordering the Commission to suspend all data flows resulting from its use of Microsoft 365 to Microsoft and its affiliates and sub-processors located in third countries not covered by an adequacy decision and to demonstrate effective implementation of such suspension. Other measures included obliging the Commission to conduct 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 any onward transfers.

## Improvements and Actions Taken

Following the EDPS's Decision, various notable improvements were made and steps taken by the Commission to ensure compliance.

Regarding purpose limitation, the Commission identified the types of personal data processed and the purposes of processing relating to its use of Microsoft 365, also making sure that Microsoft and its sub-processors process personal data only on documented instructions for specified public interest purposes. Any further processing is now performed, within the EEA as mandated by applicable EU or Member State law, or outside the EEA as decreed by third-country law that ensures essentially equivalent protection to the protection provided within the EEA.

The Commission has also made improvements to its international personal data transfers practices, specifying the particular purposes and recipients for which personal data in its use of Microsoft 365 may be transferred and guaranteeing compliance with the rules on transfers on the basis of adequacy decisions. Both the Commission and Microsoft have also introduced technical and organisational measures which limit potential transfers of personal data to third countries not covered by adequacy decisions. Transfers outside of the EU/EEA have also been restricted to certain specified countries (such transfers either benefit from adequacy decisions or rely upon the exemption for significant public interest reasons). The Commission has also provided Microsoft and its sub-processors with mandatory directions in this regard.

In respect of disclosures and notifications, further contractual obligations make certain that only EU or Member State law may require Microsoft or its sub-processors not to inform the Commission of disclosure requests for personal data regarding the Commission's use of Microsoft 365 processed inside the EEA, or that they disclose such data. Regarding non-EEA countries, the same may be required under third-country law, provided it ensures essentially equivalent protection.

## Comment

This investigation has highlighted how all organisations need to regularly review their data handling practices, and technology vendor contracts, and not assume they are compliant with data laws. Even the European Commission was found to be in breach and had to take significant steps, working with the EDPS and Microsoft, to remedy the numerous issues.

As Wojciech Wiewiórowski, Supervisor, noted "*Thanks to our thorough investigation, and the Commission's follow-up, we have jointly contributed to a significant improvement of data protection compliance in the Commission's use of Microsoft 365. We also acknowledge and appreciate Microsoft's efforts to align with the Commission's requirements stemming from the EDPS decision of March 2024.*"

While good news for now for the Commission, the EDPS made it clear that the recent enforcement proceedings were limited to certain provisions of the Regulation only and that the conclusion of the proceedings does not suggest that the EDPS considers the Commission to be compliant with all aspects of the Regulation. In view of this, the Commission is unlikely to relax its efforts to ensure compliance with the Regulation in all respects.

The Decision and enforcement proceedings in respect of the Commission also send a clear message to other EUIs using, or thinking of using, Microsoft 365. The EDPS has applauded the Commission's decision to provide other EUIs with details of the latest updates to the Inter-Institutional Licensing Agreement with Microsoft and has urged any EUI's that are using, or planning to use, Microsoft 365 services to evaluate such use and to take any necessary steps to ensure that all relevant requirements of the Regulation are complied with.

While the recent proceedings have underlined the fact that EUIs should take care to ensure that they lead by example when it comes to the protection of personal data, it should also be noted that private organisations, as well as public institutions, cannot afford to rest on their laurels when it comes to data protection compliance, whether generally or in the context of their cloud services arrangements. Private companies should learn from the lessons provided by the Commission's recent experiences and scrutinize their agreements with cloud service providers, particularly in respect of the rules around purpose limitation, international data transfers and data subject rights under the GDPR and the UK GDPR.

## Contacts

**Rafi Azim-Khan**
Partner
London D | +44.20.7413.1307
San Francisco D | +1.415.365.7282
rafi@crowell.com

**Emma Wright**
Partner
London D | +44.20.7413.1315
ewright@crowell.com

**Clare Sellars**
Counsel
London D | +44.20.7413.1309
csellars@crowell.com

**Grace Tang**

 

Associate
London D | +44.20.7413.1353
gtang@crowell.com

 