REMINDER

ONGOING INVESTIGATION INTO THE USE OF M365 BY EUIS AFTER SCHREMS II

February 2022

When EU institutions, bodies, offices and agencies ("EU institutions") procure tools with which they will process personal data or when they engage the services of processors to process personal data on their behalf, EU institutions bear legal obligations as the controller of that processing. EU institutions must ensure that the whole chain of processing by them and on their behalf will meet the requirements of Regulation 2018/1725 and ensure the protection of the rights of data subjects. In line with the principles of data protection by design and by default (the respect of which is an obligation in accordance with Article 27 of Regulation 2018/1725), EU institutions must consider the most data protection and privacy-friendly solutions.

The EDPS has an **ongoing investigation into Commission's use of Microsoft Office 365** (M365). While the ongoing investigation by the EDPS concerns the Commission in its capacity as a controller for its use of M365, the future outcome of this investigation should nevertheless be instructive for other EU institutions (EUIs) procuring of Microsoft products and services under the same inter-institutional licensing agreement with Microsoft.

The 2020 recommendations of the EDPS for EUIs' use of Microsoft products and services

Following our **2019-2020 investigation into the EU institutions' use of Microsoft products and services, the EDPS found a number of concerning areas of non-compliance**, such as incompliant data processing agreement, lack of control over use of sub-processors, lack of audit rights, lack of control over location of data processing and what was transferred out of the EEA and how, as well as a lack of proper safeguards to protect data that left the EEA. In our 2020 investigation report, we made a number of recommendations to the EU institutions, including that the EU institutions should **renegotiate their licence agreement** and put in place contractual terms to clarify amongst others how to protect data being transferred. We made clear that - unless our recommendations were implemented - the contract with Microsoft should require that **any processing of any personal data entrusted to Microsoft or its sub-processors by EU institutions *should as a rule* take place within the Union or European Economic Area**. Moreover, we recommended that EU institutions should consider carefully any purchases of Microsoft products and services or new uses of existing products and services until after they have analysed and implemented the recommendations in the report. Where EU institutions planned to use Microsoft products and services they did not already use (such as Microsoft Office 365 or Microsoft Azure cloud services), they should perform comprehensive assessments of the data protection risks posed by those products and services prior to deploying them.

Transfers outside the EEA post Schrems II and ongoing EDPS investigation

Following the ruling in the **Schrems II Judgment**, transferring personal data to non-adequate third countries, and notably to the US, has become difficult. The Judgment has far-reaching consequences on all legal tools used to transfer personal data from the EEA to any third country and in particular to the United States. **Merely using standard or ad hoc contractual clauses is not sufficient to ensure an essentially equivalent level of protection as in the EU.** This is why in its Order of 2 October 2020 and its **Strategy for EU institutions to comply with the Schrems II ruling**, the **EDPS strongly advised against starting any new processing operations or new contracts with any service providers that would involve transfers of personal data to the US.**
In line with its above-mentioned Strategy, the EDPS opened in May 2021 **two investigations following the "Schrems II" Judgment**, one of which is the investigation into the Commission's use of M365. In view of the above, **until the end of the EDPS' investigation** into Commission's use of Microsoft Office 365, the EDPS is **not in a position to draw any conclusion on the compliance** of these services with Regulation 2018/1725.

Without prejudice to any findings and conclusions that the EDPS will reach in its ongoing investigation, the fact that following our 2019-2020 investigation, the EDPS opened in 2021 another investigation into an EU institution's use of M365, should be an indication to other EUIs that the EDPS still has concerns about the inter-institutional licensing agreement for Microsoft products and services. All the more so since the Schrems II Judgment was issued. Our starting point is to check the Commission's compliance with the recommendations previously issued by the EDPS on the use of Microsoft products and services by EU institutions, including as regards location of data, international transfers and unauthorised disclosures of data, taking into account the Schrems II Judgment. Following the Judgment, Microsoft announced new measures with the aim to align themselves with the Judgment. We have concerns that these announced measures may not be sufficient to ensure full compliance with EU data protection law when EU institutions use these cloud services.

This being said, **it is a good reflex for EUIs as controllers of the processing by and on their behalf to start considering limiting processing to the EU** (using the same or alternative service providers), as in many situations it would be difficult to find effective supplementary measures to ensure the required level of protection. In that respect, in another case the EDPS had issued a warning to one EUI, which intended to acquire a new service that is part of the M365 suite, that the processing operation envisaged by that EUI was likely to infringe Regulation 2018/1725. The EDPS considered that the measures envisaged were insufficient to mitigate the risks identified by that EUI. As a consequence, the EDPS found that there were not sufficient guarantees and appropriate safeguards that the processing by Microsoft and its sub-processors resulting from that EUI's use of that service from the M365 suite and the associated transfers of personal data to them will meet the requirements of Regulation 2018/1725 and ensure an essentially equivalent level of protection to that guaranteed in the EEA.

EDPS participation in the 2022 coordinated action of the EDPB

Use of non-compliant ICT products and services by the public sector threatens the protection of personal data of all EU residents. Public sector bodies at national and EU level have a duty to lead by example, including when it comes to outsourcing and transfers of personal data within and outside the EEA. The EDPS is participating in the **2022 coordinated action of the EDPB into the use of cloud-based services by the public sector** (see press release **here**). We will cooperate with other supervisory authorities on the matter, in particular with our supervision and enforcement actions implementing the EDPS' Schrems II strategy. A coordinated action at national and EU level to bring about improvements of compliance in services provided to the public sector is likely to lead also to meaningful change in the EU market.