



PRESS RELEASE

EDPS/2022/05
Brussels, 18 February 2022

Data protection and use of cloud by public sector: the EDPS initiates and participates in the 2022 Coordinated Enforcement Action of the EDPB

The [2022 Coordinated Enforcement Action](#) (CEF) of the European Data Protection Board (EDPB) officially kicked off on 15 February 2022 with a series of actions that will be taken by the 22 participating supervisory authorities competent at national and EU level. Building on common preparatory work by all participating supervisory authorities, the authorities will implement the CEF at their level in one or several of the following ways: fact-finding exercise; questionnaire to identify if a formal investigation is warranted; commencement of a formal investigation; follow-up to ongoing formal investigations.

The European Data Protection Supervisor (EDPS) is participating in the 2022 coordinated action of the EDPB by focusing on the EU institutions', bodies', offices' and agencies' compliance with [Regulation \(EU\) 2018/1725](#) when using cloud-based services. This topic was first proposed by the EDPS in light of the need for closer cooperation and action to ensure compliance with EU data protection laws, in particular regarding the controller-processor relationship and international transfers when public sector bodies use cloud-based services.

Wojciech Wiewiórowski, EDPS, said: *“It is important that organisations within the public sector at national and EU level lead by example when it comes to outsourcing services and transferring personal data within and outside the EEA, by continuously putting in place effective measures to protect individuals’ personal data according to EU standards. A coordinated action at national and EU level, launched by the European Data Protection Board, plays an important role in ensuring that cloud-based services are fully compatible with EU data protection laws. I look forward to cooperating with other supervisory authorities, by building on the experience set out in the [EDPS’ Schrems II Strategy](#)”.*

The results of the actions by the participating supervisory authorities in the context of the 2022 coordinated action will be analysed in a coordinated manner and the participating authorities will decide on possible further supervision and enforcement actions at their level. In addition, results will be aggregated, generating deeper insight into the topic and allowing targeted follow-up by the EDPB. The EDPB will publish a report on the outcome of this analysis before the end of 2022.

Background information

On 20 October 2020, the European Data Protection Board (EDPB), decided to set up a [Coordinated Enforcement Framework](#) (CEF). The CEF is a key action of the EDPB under its [2021-2023 Strategy](#), together with the creation of a Support Pool of Experts (SPE). The two initiatives aim to streamline enforcement and cooperation among supervisory authorities.

On [7 July 2021](#), the EDPB discussed possible topics for its first coordinated enforcement action. The EDPB decided that the first action would concern the use of cloud-based services by public sector bodies. This topic was first proposed by the European Data Protection Supervisor (EDPS) in light of the need for closer cooperation and action to ensure compliance with EU data protection laws, in particular with regard to the controller-processor relationship and international transfers when public sector bodies use cloud-based services.

On [13 October 2021](#), the EDPB decided to launch this first coordinated enforcement action concerning the use of cloud-based services by the public sector and further work was carried out to specify the details and the scope of such coordinated action.

The EDPS participation in the coordinated action is based on **ongoing supervision and enforcement activities of the EDPS**, in particular those implementing the [EDPS' Strategy for EUs to comply with the Schrems II ruling](#). The EDPS for example has [two ongoing investigations into EUs' use of cloud-base services](#) that it opened following the Schrems II Judgment. The EDPS will **exchange information** gathered in our investigations and other cases, our **understanding of the issues** found and any **examples of best practices** with the authorities participating in the 2022 coordinated action.

According to EuroStat, the cloud uptake by enterprises doubled across the EU in the last 6 years. The COVID-19 pandemic has sparked a digital transformation of organisations, with many public sector organisations turning to cloud technology. However, in doing so, public bodies at national and EU level may face difficulties in obtaining Information and Communication Technology (ICT) products and services that comply with EU data protection rules. Public sector bodies in EU Member States and the EU institutions, bodies, offices and agencies (EUIs) are controllers for the processing of personal data, who typically process the data based on a legal obligation, in the performance of their tasks carried out in the public interest or in the exercise of their official authority, as they are laid down by EU or Member State law. Use of non-compliant ICT products and services by the national and EU public sector threatens the protection of personal data of all EEA residents.

While supervisory authorities carried out [actions](#) before the EU data protection reform regarding the compliance of different products and services used in the private sector, the work (by national supervisory authorities (e.g. [Belgian](#) or [German authorities](#)) and by the EDPS) regarding the use in the public sector after the adoption of the GDPR and Regulation (EU) 2018/1725 showed that compliance concerns remain. Even more so after the [Schrems II Judgment](#) of the Court of Justice of the EU. The outcome of [the 2019-2020 EDPS investigation](#), the decisions by the [French Conseil d'Etat](#), the analysis by [German supervisory authorities](#), decision of the [Portuguese supervisory authority](#) etc. have generated considerable attention to compliance of the use of cloud services by public sector bodies.

Coordinated guidance and action by the supervisory authorities competent at EU Member State and EU level is necessary to bring about meaningful change in the market. Initiatives, such as [The Hague Forum](#) (proposed by the EDPS and the Dutch Ministry of Justice and Security (Strategic Vendor Management Microsoft)), have demonstrated that meaningful progress can be made when customers of the public sector unite to negotiate better terms for cloud services. Moreover, any improvements of compliance in services provided to the public sector is likely to also lead to improvements in services provided to the private sector. The [2020 public consultation of the EDPB controller-processor guidelines](#) clearly showed that many stakeholders are concerned by the fact that they have little or no bargaining power to alter the standard terms imposed by major providers of cloud services.

The rules for data protection in the EU institutions, as well as the duties and powers 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 on to serve a five-year term, beginning on 6 December 2019.

About EDPS investigations: We conduct investigations on our own initiative or on the basis of a [complaint](#). We have extensive powers to access all personal data, information and documents, which are necessary for our investigations, and to access premises, including any data processing equipment and means, in case an on-site investigation is needed. An investigation can be of a general nature, such as our survey on compliance with data protection rules in the EU institutions, which we conduct every two years. We also conduct more targeted investigations on specific subjects, for instance, video surveillance in the EU institutions. More information can be found on the EDPS website here.

About the “Schrems II” Judgment: Following the “Schrems II” Judgment, on 29 October 2020 the EDPS issued his strategic document aiming to monitor compliance of European institutions, bodies, offices and agencies (EUIs) with the [“Schrems II” Judgment](#) in relation to transfers of personal data to non-EEA countries, and in particular to the United States. The goal is that ongoing and future international transfers are carried out in accordance with EU data protection law. In his Strategy, the EDPS

developed an action plan to streamline compliance and enforcement measures, distinguishing between short-term and medium-term compliance actions. More information can be found on the EDPS website [here](#).

About transfers of personal data: The European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) cooperate closely on matters of data protection, including on transfers of personal data. They issued [joint opinions](#) on the proposals for standard contractual clauses for contracts between controllers and processors and on the standard contractual clauses for the transfer of personal data to third countries, which were later adopted by the Commission on [4 June 2021](#). The EDPB, with the EDPS' active cooperation, issued Recommendations 01/2020 on supplementary measures to ensure an essentially equivalent level of protection in the EU/EEA when transfers of personal data to non-EU countries occur, which can be found on the EDPB website [here](#).

Personal data: [see EDPS Glossary](#)

Processing personal data: [see EDPS Glossary](#)

Privacy: the right of an individual to be left alone and in control of information about his or herself. The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7). The Charter also contains an explicit right to the protection of personal data (Article 8).

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 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

