PRESS RELEASE

EDPS/2022/13
Brussels, 18 May 2022

EDPS welcomes much-needed harmonised rules on cybersecurity and information security for all EUIs.

On 17 May 2022, the EDPS published two Opinions, one on the Proposal for a Regulation laying down measures for a high common level of **cybersecurity** in the EU institutions, bodies, offices and agencies (EUIs) ('Cybersecurity Proposal') and one on the **information security** in the EUIs ('Information Security Proposal'').

The EDPS welcomes the aim of the Proposals to improve the cybersecurity and information security of EUIs, by establishing **common rules and minimum-security requirements** that are aligned with relevant objectives of the **EU's Cybersecurity Strategy**. Both Proposals are interlinked with the NIS 2.0 Proposal , which aims to harmonise and strengthen cybersecurity practices across the European Union, and for which the EDPS had issued an Opinion.

Wojciech Wiewiórowski, EDPS, said: *"With the NIS 2.0 Directive just agreed by the co-legislators last week, the European Commission has gone one step further by proposing corresponding rules for EUIs in a timely manner. These will be the first legal acts devoted exclusively to regulating data security in the EUIs, including at the EDPS. There is no protection of personal data without effective security risk management and measures. At the same time, it is essential to protect personal data processed in the information security and cybersecurity contexts. I believe the texts provide a good basis, but can be improved with more assurances for the rights and freedoms of individuals when their data is processed in security operations."*

In his Opinions, the EDPS stresses how these Proposals can **also** have a **positive impact on the security of personal data,** as mandated by Regulation (EU) 2018/1725. At the same time, he highlights the **risks for compliance** with the EU privacy and data protection legislation that are implied by the security measures mandated by the Proposals. In this respect, the EDPS recommends ensuring that all security measures envisaged have a valid legal basis, be necessary and proportionate.

In order to comply with both Proposals, the EUIs, as well as CERT-EU, which is acting as the 'Cybersecurity Centre' of the EUIs, will have to deploy processes and measures implying additional processing of personal data. To **achieve legal certainty and foreseeability, and to ensure compliance with Regulation (EU) 2018/1725,** the EDPS strongly advises that both Proposals provide a clear, legal ground for the processing of personal data by CERT-EU and the EUIs, including, in particular, the purposes of processing and the categories of personal data that may be processed.

The EDPS believes that the Cybersecurity Proposal, in particular, needs to be improved **to align** with the substantive rules of the NIS 2.0 Directive, so that **consistent and homogeneous rules for EU Member States and the EUIs** are achieved, to contribute to the overall Union cybersecurity level.

As already stated in his NIS 2.0 Opinion, the EDPS stresses the importance of **integrating the privacy and data protection perspective in the management of cybersecurity and information security**, in order to achieve positive synergies. Moreover, he provides specific recommendations on how such synergies can be achieved by the Proposals, including a specific obligation for EU officials responsible for cybersecurity and information security to cooperate closely with the data protection officers, integration of the security risk management with personal data security, and integration of security incident and data breach handling procedures.

The EDPS **strongly advises** that the Cybersecurity Proposal provides for the **EDPS' participation** in the 'Interinstitutional Cybersecurity Board'. He also believes that the Proposal should provide for **close cooperation between CERT-EU and EDPS**.

Background information

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

The EDPS is the independent supervisory authority with responsibility for monitoring the processing of personal data by the EU institutions and bodies, advising on policies and legislation that affect privacy and cooperating with similar authorities to ensure consistent data protection. Our mission is also to raise awareness on risks and protect people's rights and freedoms when their personal data is processed.

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.

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