European Data Protection Board

Anu Talus
Chair of the European Data Protection Board

European Union Agency for Cybersecurity
Agamemnonos 14,
Chalandri 151231,
Greece

Brussels, 16 July 2024

by email only

Subject: EU cybersecurity certification scheme on cloud services supporting compliance to GDPR and cooperation options regarding the eHealth sector - EDPB reply letter

In your letter of 11 March 2022, you had proposed to work together "to draw up, for instance, common cybersecurity requirements related to data protection into a dedicated extension profile, and guidance relative to data protection for both CSPs and cloud customers". As a follow up, between September 2022 and January 2024, ENISA representatives participated in EDPB experts' subgroup meetings to discuss the matter, and they responded to a questionnaire sent by the EDPB. I would like to thank you for this fruitful collaboration.

The EDPB finds that several important issues related to the links between the cybersecurity risk assessment in the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and personal data protection risk assessment need to be addressed. Although the EUCS necessitates compliance with the law, it is not clear how, for example, the assurance levels of EUCS scheme may be mapped with usage scenarios involving personal data - which in turn poses questions on whether adoption of cybersecurity certification suffices to ensure appropriate security measures for a certification pursuant to the art. 42 of the GPDR.

The EDPB suggests to work together with ENISA by establishing a joint ad-hoc working group with the task to explore and assess the following possible objectives:

- Draw up guidance relative to data protection for both CSPs and cloud customers (e.g. map the assurance levels of EUCS scheme with usage scenarios involving personal data, or clarify that some of them can be flagged as generally non-sufficient for the processing of personal data).
- Assist DPAs, GDPR Certification scheme owners, or GDPR Codes of Conduct owners to articulate GDPR tools (certification, code of conduct, etc.) with the EUCS scheme

European Data Protection Board
Rue Wiertz, 60
1047 Brussels

- Develop a risk assessment methodology in order to assess the circumstances in which the EUCS assurance levels escalate along with the data protection risks, and to check whether the security measures envisaged in each of the EUCS assurance levels mitigate (and to what extent) the associated data protection risks
- Create an EUCS dedicated extension profile covering GDPR related additional requirements

We are therefore open to discuss and explore with you the appropriate shape and form of this collaboration.

Yours sincerely,

Anu Talus

European Data Protection Board
Rue Wiertz, 60
1047 Brussels