edpb
European Data Protection Board

Letters

European Union Agency for Cybersecurity
Athens, Greece

Brussels, 09 March 2021
Ref: OUT2021-0047

ENISA published a draft version of the candidate European Cybersecurity Certification Scheme for Cloud Services (EUCS) on 22 December 2020. Following the publication, ENISA launched a public consultation on the draft scheme. The EDPB takes this opportunity to provide feedback on the EUCS candidate scheme, more specifically in relation to the potential synergies between the EUCS scheme with a view to supporting Cloud Service Customers (CSC) and Cloud Service Providers (CSP) to comply with the principles and rules established in the Regulation (EU) 2016/679 (GDPR)[1] with regard to the protection of personal data.

On the one hand, in accordance with Regulation (EU) 2019/881 (Cybersecurity Act)[2], cybersecurity aims at the *protection of "network and information systems, the users of such systems, and other persons affected by cyber threats"*, thereby also contributing to security of the processing of their personal data.

On the other hand, data protection rules laid down in the GDPR have as main objective the protection of natural persons with regard to the processing of their personal data. A key principle of the GDPR enshrined in article 5 (1) (f), imposes the respect of the 'confidentiality and integrity' of personal data undergoing processing. This key principle needs to be considered alongside article 32 of the GDPR that provides more specifically to the security of personal data processing.

The EDPB considers it important to identify and define synergies between the different tools that support data protection compliance and those that support information security. In this context, it is also important to ensure that the controls and requirements in the cybersecurity certification scheme do not conflict with the rules and principles of the GDPR. By doing so, adherence to these tools by the concerned stakeholders would also be facilitated.

In particular, the EDPB agrees with the approach adopted by the EUCS candidate scheme according to which the latter *"does not aim at verifying the compliance of a cloud service to any regulation beyond*

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[2] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013

the EUCSA, and in particular it does not aim at verifying compliance with GDPR". Moreover, Article 54 of the EU Cybersecurity Act states that the '*requirements of the European cybersecurity certification scheme shall be consistent with any applicable legal requirements*'. Furthermore, the EDPB also acknowledges the candidate scheme could contribute to facilitate compliance with the GDPR, i.e. in securing personal data processed by the cloud service provider, in line with the 'confidentiality and integrity' principle as per Article 5 (1) (f) GDPR.

The EDPB also welcomes the EUCS certification scheme initiative as tool to harmonize the security of cloud computing services at European level. The EUCS scheme will furthermore improve transparency on guarantees for security measures provided by a cloud service for public institutions, private companies and indirectly customers.

1. Personal data processing under the GDPR and security requirements

The EUCS scheme provides for a definition of "*cloud service customer data*", "*cloud service derived data*" and "*cloud service provider data*" as classes of data objects categorized into non-critical, business critical and mission critical information.

In this regard, the EDPB recalls that Article 4 (1) GDPR provides for the definition of *"personal data*"[3]. Article 9 GDPR moreover defines the concept of *"special categories of personal data*"[4]. The latter is comprised of personal data, which are by their nature, particularly sensitive in relation to the fundamental rights and freedoms of natural persons and merit higher protection and security.

In light of the above, the EDPB notes that the EUCS scheme introduces classes of data objects that may include personal data, without referring to the concepts of personal data and special categories of personal data defined in the GDPR. Moreover, the EUCS scheme assurance levels are intended to minimize known basic risks of incidents and cyber-attacks up to risks of state-of-the-art cyberattacks carried out by actors with significant skills and resources, while data controllers are also required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk for the rights and freedoms of natural persons and taking into account the scope, context and purpose of the processing in order to comply with Article 32 GDPR (Security of processing).

Therefore, and since the risk inherent in processing of personal data is of varying likelihood and severity for the rights and freedoms of natural persons depends amongst others on the category of personal data processed, the inclusion of personal data and special categories of personal data into the EUCS scheme is even more critical.

---

[3] According to Article 4 (1) GDPR, "'*personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

[4] Article 9 (1) GDPR defines special category data as "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), data concerning health, a person's sex life and data concerning a person's sexual orientation*".

Recommendation 1:

In order to provide an added value to the EUCS scheme and to ensure that -insofar as personal data are concerned- no inconsistencies with the definitions and concepts of the GDPR occur the EDPB suggests to introduce personal data and special categories of personal data as categories of data into the EUCS scheme, taking into account that derived data (not directly provided by data subjects) may be personal data. These two categories of data should also be taken into account to guide CSPs and CSCs when applying for an appropriate assurance level.

To further support the compliance with GDPR obligations by CSCs, and depending on the cloud capability type, the CSP may already be aware of the processing of personal data taking place in its cloud service. For example, an application cloud service, may process personal data as part of the service offered to the CSC (e.g. online HR software). For this type of service, the CSP should offer a level of security already adapted to the risks of this particular personal data processing and therefore have a certification with a level of assurance adapted to its context. Indeed, the GDPR requires processors to assist controllers[5] in ensuring compliance with the obligations pursuant to Articles 32 taking into account the nature of processing and the information available to the processor.

Recommendation 2:

The EDPB suggests that the EUCS scheme encourages CSPs to choose for their certification a level of assurance that already takes into account, where applicable, the type of personal data likely or intended to be processed and the risks to the rights and freedoms of natural persons resulting from the processing carried out.

2. **The differences between data protection rights (the right to data portability) and principles (confidentiality, integrity, transparency) and the security objectives (confidentiality, integrity, transparency, portability) in the EUCS candidate scheme**

The EDPB also wants to stress the importance of the principles relating to processing of personal data set forth by Article 5 GDPR. Adequate security of personal data, mentioned in article 5 (1) (f) GDPR as the principle of 'integrity and confidentiality', is only one of them. Other principles must be considered when processing personal data, such as 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimization', 'accuracy', 'storage limitation' and 'accountability'.

For instance, in relation to the principle of transparency, the EDPB welcomes the inclusion of the "Complementary Customer Controls"[6], according to which a CSP must provide information about the location of the processing and storage of data as well as the applicable law. Such information might help the CSC who wants to process personal data in the context of cloud computing services provided

[5] Allocation of responsibilities for personal data processing in the context of cloud services has to be assessed on a case by case basis. The current EDPB guidelines on controller and processor in the GDPR can be found here:
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf
[6] Control DOC-03 LOCATIONS OF DATA PROCESSING AND STORAGE (pg. 151 of EUCS)

by the CSP to comply with security requirements and comply with the requirements of GDPR, especially with regard to the transfers of personal data to third countries[7].

Recommendation 3:

The EDPB recommends including the requirements about the location of data processing in all assurance levels. Not including these requirements in the basic assurance level, as it is currently the case, would exclude this assurance level of the EUCS scheme to facilitate the compliance with GDPR for any personal data processing.

The principles mentioned above should guide all processing activities concerning personal data and are of particular relevance to allow data subjects to have control over the personal data relating to them, especially through the exercise of their rights as data subjects under the GDPR. For instance, the right to portability further strengthens the control of the data subjects over the personal data relating to them, by allowing them to receive personal data concerning them in a structured, commonly used, machine-readable and interoperable format, and to transmit those data to another controller. The high level of portability that can be achieved by the cloud service providers certified under EUCS candidate scheme meets different requirements than the right of portability in the GDPR.

Recommendation 4:

Therefore, the EDPB suggests clearly indicating in the scheme that the portability control in the EUCS scheme should not be confused with the right of portability in the GDPR.

The mandate received by ENISA to develop the EUCS candidate scheme is based on Article 54 of the EU Cybersecurity Act. This article states that the *'requirements of the European cybersecurity certification scheme shall be consistent with any applicable legal requirements*'. These legal requirements include the compliance with the data protection *acquis* when the cloud service provided by the CSP involves the processing of personal data.

Recommendation 5:

In this regard, the EDPB recommends the involvement of the CSP's Data Protection Officer (DPO) in the early stages of the designing of the service to assist the CSP to monitor internal compliance with the GDPR. By doing so, the security by design of the cloud service will be reinforced by contributing to the obligation of 'data protection by design'.

[7] See, for example, Articles 13 (1) (f), 14 (1) (f) and 15 (2) GDPR and more generally Chapter V of the GDPR.

The EDPB namely considers that the advice provided by the DPO to the CSP is an element that can positively contribute to the adoption of appropriate technical and organisational measures to safeguard the rights and freedoms of natural persons in the context of the EUCS candidate scheme and to ensure the consistency with the applicable legal requirements established by the EU Cybersecurity Act.

3. Extension of the audit rights for data controllers / processors

The EDPB welcomes that "*the CSP shall grant its CSCs contractually guaranteed information and define their audit rights*".

Recommendation 6:

The EDPB recommends envisaging this possibility not only for the "High level" of assurance, but also for the "Basic" and for the "Substantial" levels of assurance. Not including this requirement in the "Basic" and "Substantial" assurance levels would exclude these assurance levels of the EUCS scheme from facilitating compliance with GDPR Article 28 (3) (h).

Therefore, it is also important to ensure that this possibility is clearly mentioned in the contract governing the provision of the cloud services between the CSP and the CSC, especially if it involves the processing of personal data. Not including this requirement in the "Basic" and "Substantial" assurance levels would exclude these level of certification to be used to facilitate compliance with Article 28 (3) (h) GDPR.

4. The EUCS scheme incident management requirements as support to the GDPR data breach requirements

Article 4 (12) GDPR defines a personal data breach as a "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*". The EUCS scheme requires in requirement IM-01.4 that "*The CSP shall inform the customers affected by security incidents in a timely and appropriate manner*". Article 33(2) GDPR however requires that "*the processor shall notify the controller without undue delay after becoming aware of a personal data breach*".

Recommendation 7:

The EDPB suggests adapting the wording of the EUCS requirements to reflect the GDPR requirements for personal data breaches and to make these requirements mandatory for all assurance levels of the

scheme. Not including these requirements in the "Basic" and "Substantial" assurance levels would preclude the use of these assurance levels of the EUCS scheme to facilitate compliance with GDPR Article 33 (Notification of a personal data breach to the supervisory authority).

5. The EUCS scheme as facilitator for GDPR Codes of conduct / certifications

By relying on a cybersecurity certification scheme harmonized at the European level, the private and public organizations that elaborate European or national codes of conduct or certification schemes, in accordance with Articles 40 and 42 GDPR, may support the applicants in demonstrating their compliance with such GDPR accountability tools. In particular, for applicants that rely on those GDPR accountability tools for the purpose of demonstrating compliance with the GDPR of their processing operations, the EUCS certificate or the related audit report may facilitate their assessment when identical or similar criteria are used in both tools.

Additionally, the EUCS scheme permits under certain conditions its assessment to a simplified methodology based on a self-assessment performed by the CSP. In this methodology, a conformity assessment body (CAB) can then audit the results of the self-assessment. As a consequence, if CSPs apply for a GDPR accountability tool that makes reference to some criteria of the EUCS scheme, the compliance to these criteria would need to be reassessed by a certification body or a monitoring body accredited, respectively, under Article 41 or 43 GDPR.

Recommendation 8:

Therefore, the EDPB suggests that all levels of the EUCS can benefit from equivalent proofs of compliance by allowing a fully independent third-party assessment. Not including this requirement would exclude the EUCS certificates or audit report based on the self-assessment methodology to facilitate compliance with GDPR accountability tools.

Conclusion

The EUCS certification may help supporting data protection security requirements and facilitate the adoption of this tool by stakeholders by:

- introducing a personal data category in the EUCS scheme;
- taking into account the notion of risks of personal data processing to the rights and freedoms of natural persons;
- reinforcing the EUCS security requirements needed to comply with the data protection rules on the security of processing;
- including in all assurance levels the GDPR security requirements mentioned in this letter. Excluding these requirements from some assurance levels of the EUCS scheme would result for the concerned assurance levels to not be usable to support compliance with GDPR requirements.

The above suggestion has only to be considered as a preliminary guidance. Assessments of the risks for personal data processing have to be done on a case-by-case basis under the responsibility of the data controller. Indeed, the GDPR accountability principle requires data controllers to take responsibility for what they do with personal data and how they comply with the all the GDPR principles.

The EDPB remains open to any further discussion elaborating on how the EUCS certification scheme could contribute to facilitate compliance with the GDPR.

Yours sincerely,

Andrea Jelinek

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels