

EDPS Formal comments on the draft Commission Delegated Regulation supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ('EUDPR')¹, and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING FORMAL COMMENTS:

1. Introduction and background

1. On 23 October 2023, the European Commission consulted the EDPS on the draft Commission Delegated Regulation supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows ('the draft delegated regulation').
2. The objective of the draft delegated regulation is to establish a recurrent process of cybersecurity risk assessments in the electricity sector². The governance model set out by the draft delegated regulation follows the objective of harmonising and ensuring a common baseline while respecting existing practices and investments as much as possible³. Further components of the draft delegated regulation are, among others, the promotion of a common electricity cybersecurity framework fostering a common minimum electricity cybersecurity level across the EU, and establishing rules for the collection and sharing of information in relation to cross-border electricity flows, compatible with other national and EU legislation⁴.

¹ OJ L 295, 21.11.2018, p. 39.

² Explanatory Memorandum, p. 1.

³ Explanatory Memorandum, p. 1.

⁴ Explanatory Memorandum, p. 2.

3. The draft delegated regulation is adopted pursuant to Article 59(2), point (e) of Regulation (EU) 2019/943⁵.
4. The present formal comments of the EDPS are issued in response to a consultation by the European Commission pursuant to Article 42(1) of EUDPR. The EDPS welcomes the reference to this consultation in Recital 31 of the draft delegated regulation.
5. These formal comments do not preclude any additional comments by the EDPS in the future, in particular if further issues are identified or new information becomes available, for example as a result of the adoption of other related implementing or delegated acts⁶.
6. Furthermore, these formal comments are without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Article 58 of the EUDPR and are limited to the provisions of the draft delegated regulation that are relevant from a data protection perspective.

2. Comments

7. The EDPS notes that the draft delegated regulation makes reference to several cybersecurity measures that are likely to entail processing of personal data. According to the information provided by the Commission, however, the draft delegated regulation does not seek to impose specific obligations to collect, process, store or exchange personal data. For example, Article 32(2) point (a) of the draft delegated regulation mentions background verification checks of certain staff as a field for recommendations within the context of minimum cybersecurity controls in the supply chain. However, the precise subject matter and extent of the background checks would be dependent on relevant laws, regulations and ethics.
8. Article 37(1) point (a)(i) obliges high-impact and critical-impact entities to ensure logging for security purposes to enable the detection of anomalies and collect information on cybersecurity incidents. The EDPS recalls that some cybersecurity measures, including logging any machine-user interactions, may involve the processing of personal data. However, the draft delegated regulation, while listing logging among the mandatory measures, does not specify the details of this obligation.

⁵ Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast), OJ L 158, 14.6.2019, p. 54.

⁶ In case of other implementing or delegated acts with an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data, the EDPS would like to remind that he needs to be consulted on those acts as well. The same applies in case of future amendments that would introduce new or modify existing provisions that directly or indirectly concern the processing of personal data.

9. The draft delegated regulation also refers to information sharing in many of its articles, for instance in Article 37(1), Article 45(7) and (8), and Article 46(7). While this information relates to security threats or incidents and do not necessarily contain personal data, Article 37(6) indicates that IP addresses may be among the reportable information. Article 37(6) of the draft delegated regulation moreover makes the presence of ‘information such as compromised URL or IP addresses, hashes or any other attribute useful to contextualise and correlate the attack’ one of several alternative preconditions for reportability.
10. Recital (30) of the draft delegation confirms that any processing of personal data in the context of this regulation is to be in accordance with the GDPR and EUDPR. While the draft regulation does not intend to regulate the processing of personal data as such, it may effectively require processing of personal data where it is incidentally embedded within the type of information required under Article 36 and 37.
11. Against this background, the EDPS recommends to clarify in which instances the draft delegated regulation aims to provide a legal basis within the meaning of Article 6 GDPR and Article 5 EUDPR. Where it is not the case, the entity deploying the measure may be able rely to on another legal basis, for example Article 6(1)(f) GDPR. It should be made clear, however, that in those cases the delegated regulation does not establish a legal obligation nor other lawful basis to process personal data.
12. In cases where the draft delegated regulation does aim to provide a lawful basis for the processing, it should clearly define both the purposes of the processing and the categories of personal data that may be processed, as well as the retention period for those data. It should also clearly assign the roles of the various actors involved as controller, joint controller or processor.
13. Finally, the EDPS welcomes the efforts undertaken with this draft delegated regulation to avoid potential conflicts with data protection law and to require anonymization, where appropriate, for example in Article 45(7)(b).

Brussels, 17 November 2023

(e-signed)

Wojciech Rafał WIEWIÓROWSKI