Formal comments of the EDPS on the Commission Implementing Decision laying down a model security plan, a model business continuity and a disaster recovery plan pursuant to Article 59(4) of Regulation (EU) 2018/1240

1. Introduction and background

The European Travel Information and Authorisation System (ETIAS) has been established by Regulation (EU) 2018/1240[1] and requires all visa-exempt third country nationals to apply online for travel authorisation prior to the date of their departure to the Schengen area.

Pursuant to Article 59(4) of the Regulation (EU) 2018/1240 the European Commission has been empowered to adopt a model security plan and a model business continuity and disaster recovery plan by means of implementing acts. The model plans adopted by the Commission shall serve as a basis, adjusted as necessary, to eu-LISA's Management Board, the European Border and Coast Guard Agency's Management Board and the Member States when adopting their own security plans and business continuity and disaster recovery plans ensuring the security of the ETIAS Information System.

The present formal comments of the EDPS are issued in response to the legislative consultation by the European Commission of 15 April 2021, pursuant to Article 42(1) of Regulation 2018/1725[2]. In this regard, the EDPS welcomes the reference to this consultation in Recital 9 of the draft Implementing Decision.

The EDPS wishes to stress that these formal comments do not preclude any future additional comments by the EDPS, 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 acts, pursuant to Regulation (EU) 2018/1240. 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 Regulation (EU) 2018/1725.

[1] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, OJ L 236, 19.9.2018, p. 1–71.
[2] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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, OJ, 21.11.2018, L.295, p.39 (Regulation (EU) 2018/1725).

2. Comments

The EDPS notes the fact that the draft Annex to the Commission Implementing Decision contains a guide to the methodology on how to write a model security plan, a model business continuity and a disaster recovery plan. However, only Appendix 10 of the Annex to the draft Commission Implementing Decisions qualifies fully as a "Model Plan".

The EDPS recalls that Article 59(2) and (3) of Regulation (EU) 2018/1240 regulate security measures "without prejudice to Article 22 of Regulation (EC) No 45/2001", subsequently replaced by Article 33 of Regulation (EU) 2018/1725, and also without prejudice to Regulation (EU) 2016/679[3]. This means that the requirements for setting up security measures in the draft Commission Implementing Decision are not limited only to the elements in Article 59 of Regulation (EU) 2018/1240but have also to comply with all the requirements stemming from Regulation (EU) 2018/1725 and Regulation (EU) 2016/679.

The EDPS further recalls that Article 33(1) of Regulation (EU) 2018/1725 as well as Article 32(1) of Regulation (EU) 2016/679 require a mandatory risk analysis "for the rights and freedoms of natural persons" to be included in the risk analysis by the controller or processor. Guidance on this mandatory requirement has been provided by the EDPS in his Guidelines on Security Measures for Personal Data Processing[4].

Whereas the traditional or general data security risk management measures aim at protecting network and information systems of the organisation (and the data therein), aforementioned Articles from the data protection legislation aim at protecting individuals and their rights by protecting their data. There is a difference in the assets to protect in the two activities, which might lead to different conclusions in certain circumstances.

The EDPS notes that the rights and freedoms of natural persons as an asset to be protected have not been sufficiently addressed by the model plans. For instance, the definitions of "Business Impact Assessment", "Impact analysis", "'Risk analysis", "Security plan" and others do not include a reference to the natural persons as data subjects and their rights. In the same vein, section 'C6. SECURITY CONTROLS AND PROCESSES' does not refer to the risks for the rights and freedoms of natural persons.

The EDPS recommends integrating the privacy and data protection considerations into data security risk management to ensure a holistic approach and enable synergies when managing data security and protection of the information they process without unnecessary multiplication of efforts, and invites the Commission to amend the draft Implementing Decision accordingly.

---

[3] 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 (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

[4] https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en.

The EDPS furthermore notes the fact that the document repeatedly refers to the US standard NIST 800-54 rev.4 and not the latest rev.5, the latter including 'privacy risks'. For example the newest standard NIST 800-53 rev.5 includes in the Risk Assessment (page 240) the "likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information", while this was not the case with the older rev.4 of the same standard (page 152). Several other national standards, such as the German 'BSI Grundschutz' in its latest version, also take into account the rights and freedoms of natural persons in their methodology.

The EDPS therefore recommends that the Commission, when referring to a US standard, refer to the latest NIST 800-53 rev.5 standard, which is more aligned with Article 32(1) or Regulation (EU) 2016/679, Article 33(1) of Regulation (EU) 2018/1725 respectively.

Brussels, 07 June 2021

Wojciech Rafał WIEWIÓROWSKI
(e-signed)