EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

9 November 2022

Opinion 23/2022

on the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

edps.europa.eu

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data... for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'...for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.

Wojciech Rafał Wiewiórowski was appointed as Supervisor on 5 December 2019 for a term of five years.

Under ***Article 42(1)*** *of Regulation 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data'.*

This Opinion relates to the Commission's Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.This Opinion does not preclude any future additional comments or recommendations by the EDPS, in particular if further issues are identified or new information becomes available. Furthermore, this Opinion is without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Regulation (EU) 2018/1725. This Opinion is limited to the provisions of the draft Proposal that are relevant from a data protection perspective.

Executive Summary

On 15 September 2022, the European Commission issued a Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 ('the Proposal').

The EDPS welcomes the Proposal and fully supports its general objective to improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market.

The EDPS recalls that Article 5(1)(f) GDPR has established security as one of the main principles relating to the processing of personal data. Article 32 GDPR further defines this obligation, applicable to both controllers and processors, to ensure an appropriate level of security. Therefore, the EDPS welcomes that security and data minimization principles are already embedded in the essential cybersecurity requirements enumerated in the Annex I of the Proposal. In addition, the EDPS strongly recommends including the data protection by design and by default principle in the essential cybersecurity requirements of products with digital elements.

Recital 17 provides for very important governance provisions that are not reflected in the operational part of the Proposal. Therefore, the EDPS recommends specifying in the operational part of the Proposal all the aspects related to the creation of synergies on both standardisation and certification on cybersecurity as well as synergies between this Proposal and the Union data protection law in the area of market surveillance and enforcement. Furthermore, the EDPS considers it necessary to clarify that the Proposal does not seek to affect the application of existing EU laws governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments.

The EDPS welcomes the fact that this provision acknowledges that the processing of personal data is a critical and sensitive function and might as such require the corresponding critical products with digital elements to obtain a European cybersecurity certificate under a European cybersecurity certification scheme. At the same time, the EDPS recommends clarifying in a recital of the Proposal that obtaining a European cybersecurity certification under the Proposal does not guarantee compliance with the GDPR.

Finally, the EDPS welcomes the proposed penalties, which are similar to those of the GDPR for a breach Article 32 GDPR on the security of processing, with a maximum fine of 2.5% of global annual turnover. As a result, the Proposal could serve as yet another form of protection for individuals that reside within EU Member States, in conjunction with the provisions of the GDPR.

Contents

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 natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies and on the free movement of such data ('EUDPR')[1], and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1. On 15 September 2022, the European Commission issued a Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 ('the Proposal').

2. The objective of the Proposal is to improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market[2]. In particular, the Proposal aims to set the boundary conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufactures take security seriously throughout a product's life cycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements[3].

3. To this end, the Proposal lays down[4]:

    - rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products;

    - essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;

    - essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;

[1] OJ L 295, 21.11.2018, p. 39.
[2] Recital 1 of the Proposal.
[3] Recital 2 of the Proposal
[4] Article 1 of the Proposal.

- rules on market surveillance and enforcement of the above-mentioned rules and requirements.

4. The EU framework comprises several pieces of horizontal legislation that cover certain aspects linked to cybersecurity from different angles (products, services, crisis management, and crimes). In 2013, the Directive on attacks against information systems[5], harmonising criminalisation and penalties for a number of offences directed against information systems came into force. In August 2016, Directive (EU) 2016/1148 on security of network and information systems (NIS Directive)[6] entered into force as the first piece of EU-wide legislation on cybersecurity. Its revision, resulting in the NIS2 Directive, raises the EU common level of ambition regarding the cybersecurity of ICT services. In 2019, the EU Cybersecurity Act[7] entered into force, aiming to enhance the security of ICT products, ICT services and ICT processes by introducing a voluntary European cybersecurity certification framework.

5. The present Opinion of the EDPS is issued in response to a consultation by the European Commission of 15 September 2022, pursuant to Article 42(1) of EUDPR. The EDPS welcomes the reference to this consultation in Recital 71 of the Proposal. In this regard, the EDPS also positively notes that he was previously informally consulted pursuant to recital 60 of EUDPR.

2. General comments

6. The EDPS welcomes the Proposal and fully supports its general objective to improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market.

7. The Proposal mandates that products with digital elements will only be made available on the market if they meet specific essential cybersecurity requirements for the design, development and production of these products. Moreover, the Proposal establishes obligations for economic operators in relation to these products with respect to cybersecurity. For example, it requires manufacturers to factor cybersecurity in the design and development of the products with digital elements.

8. Whereas the NIS2 Directive included in its scope of application operators of essential services and digital services providers in order to establish a high common level of cybersecurity of their ICT systems, the Proposal at hand would introduce common cybersecurity rules for manufacturers and developers of products with digital elements, covering both hardware and software. The EDPS notes that such products can be embedded in the ICT systems of digital service providers, acting as entities under NIS2 Directive and can be used by individuals that use digital services, such as mobile phones, personal

[5] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA OJ L 218, 14.8.2013, p. 8–14.
[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194/1, 19.7.2016 p. 1.
[7] 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 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15.

computers, operating systems and software applications. In this context, the EDPS recalls his Opinion on the Cybersecurity Strategy and the NIS 2.0 Directive[8].

9. Pursuant to the Explanatory Memorandum[9] the horizontal cybersecurity requirements:

    - would contribute to the security of personal data by protecting the confidentiality, integrity and availability of information in products with digital elements.

    - will facilitate compliance with the requirement of security of processing of personal data under the GDPR.

    - would enhance the transparency and information to users, including those that might be less equipped with cybersecurity skills. Users would also be better informed about the risks, capabilities and limitations of the products with digital elements, which would place them in a better position to take the necessary preventive and mitigating measures to reduce the residual risks.

10. The EDPS recalls Article 5(1)(f) GDPR has established security as one of the main principles relating to the processing of personal data. Article 32 GDPR further defines this obligation, applicable to both controllers and processors, to ensure an appropriate level of security. Therefore, the EDPS welcomes that security and data minimization principles are already embedded in the essential cybersecurity requirements enumerated in the Annex I of the Proposal.

11. The cybersecurity of products with digital elements that are used by individuals is of utmost importance to protect their rights and freedoms, in particular the right to privacy, and to enhance their trust in digital services. Without such requirements, the individuals can fall victims of cybersecurity attacks aiming to have access to their personal data and confidential communications.

12. This is why the EDPS considers that laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements is very important for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and strongly supports the Proposal for a comprehensive package of relevant effective technical and organisational measures.

13. In addition, the EDPS recalls that Article 25 GDPR lays down data protection by design and by default principle, which aims to build data protection and privacy into the design of processing operations and information systems, even before the actual processing takes place, and to ensure that by default, only personal data which are necessary for each specific purpose of the processing are processed. In practice, this principle requires, amongst others, the use of privacy enhancing technologies such as encryption and pseudonymization. The GDPR provisions make clear that security and data protection by design and by default are essential for compliance with EU data protection law.

14. Concerning the products with digital elements, the role of manufacturers is typically limited to supplying the product to individuals. The GDPR does not impose requirements on manufacturers directly, but only "encourages" them in recital 78 GDPR "*to take into*

[8] EDPS Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive, issued on 11 March 2021
[9] COM(2022) 454 final, p. 8.

account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations". Nevertheless, it is clear that users will ultimately decide against a product if using it means that they, as controllers, will be unable to adhere to data protection requirements. This creates an indirect "requirement" for manufacturers to design their products in such a way that users will be able to adhere to the requirements of the GDPR when processing data in the future.

15. Therefore, despite the fact that the GDPR does not address directly the manufacturers of products with digital elements, but only the controllers when such products are embedded in their ICT systems, it is essential that the principle of data protection by design and by default is applied also to products. On the one hand, it would facilitate the compliance of controllers with the principle of data protection by design and by default and on the other hand, it would ensure that personal data of individuals using such products in order to access digital services is duly protected. Therefore, the EDPS strongly recommends including the data protection by design and by default principle in the essential cybersecurity requirements of products with digital elements.

3. Scope of the Proposal

16. The wide scope of the Proposal covers all products with digital elements, and specifically *"means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately"*[10]... *"whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network"*[11]. This includes both products that can be connected physically via hardware interfaces and products that are connected logically, such as via network sockets, pipes, files, application programming interfaces and any other type of software interface.

17. The EDPS understands that products with digital elements under the scope of the Proposal can be embedded in the ICT systems of controllers[12] and can be used by individuals[13] in order to access personal data processing services provided by controllers.

18. In this context, the EDPS recommends explaining in the preamble to the Proposal the importance of products with digital elements that perform cryptographic operations[14] including encryption at rest and in transit and pseudonymisation that are necessary for effective information security, cybersecurity, data protection and privacy. Furthermore, in line with recital 26 of the Proposal, he also recommends adding in Annex II tangible and intangible products with digital elements that perform cryptographic operations.

19. The EDPS notes that certain digital products and services subject to sectoral legislation fall outside of the Proposal's scope. These include software-as-a-service, medical devices, *in*

---

[10] Article 3(1) of the Proposal provides that: 'product with digital elements' means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately.

[11] Article 3(2) of the Proposal provides that: "This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network."

[12] For example: hardware and operating system of servers, software of application servers, software of web applications, etc.

[13] For example: mobile phones, personal computers, operating systems, software applications etc

[14] The EDPS recalls the impact of bugs found in encryption products used by service providers and users such as the 'Heartbleed', 'POODLE', as well as the 'VeraCrypt' case.

vitro diagnostic medical devices, motor vehicles, products used exclusively for national security or military purposes or designed specifically to process classified information.

20. Nevertheless, security related provisions of some sectoral legislations excluded from the scope of the Proposal are not always as detailed and concrete as the ones in the Proposal itself. This is the case of Regulation (EU) 2017/745[15] that sets up general safety measures for medical devices, but does not require the devices to be delivered without any known vulnerabilities or to encrypt relevant data at rest or in transit according to state of the art mechanisms. Moreover, the same Regulation includes the obligation to *'establish, implement, document and maintain a risk management system'*. However, it is unclear if such system will also cover cybersecurity and data protection related aspects. In consequence, the EDPS recommends deleting Regulation (EU) 2017/745 from the list of the legislations excluded from the application of the Proposal.

21. The EDPS also notes that Recital 15 indicates that the essential requirements laid down by the Proposal 'include all the elements of the essential requirements referred to in Article 3(3), points (d), (e) and (f) of Directive 2014/53/EU on the marketing of radio equipment[16]. As point (e) refers to personal data and privacy, the EDPS recommends clarifying expressly in the Proposal what are the elements of the essential requirements referred to by Article 3(3)(e) of Directive 2014/53/EU on personal data and privacy.

4. Relationship to existing Union legislation on personal data protection

22. The EDPS observes that Recital 17 of the Proposal clarifies that it is *"without prejudice"* to the GDPR and indicates that:

    - synergies on both standardisation and certification on cybersecurity aspects should be considered through the cooperation between the Commission, the European Standardisation Organisations, the European Union Agency for Cybersecurity (ENISA), the European Data Protection Board (EDPB) established by the GDPR , and the national data protection supervisory authorities;
    - synergies between this Proposal and the Union data protection law should also be created in the area of market surveillance and enforcement. To this end, national market surveillance authorities appointed under this Proposal should cooperate with authorities supervising Union data protection law. The latter should also have access to information relevant for accomplishing their tasks.

23. The EDPS takes note that Recital 17 provides for very important governance provisions that are not reflected in the operative part of the Proposal. In addition, the way these 'synergies' could be created is not detailed. The EDPS is concerned that such synergies are unlikely to occur in practice in the absence of clear corresponding provisions,Therefore, the EDPS

[15] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, JO L 117 du 5.5.2017, p. 1–175.

[16] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance, OJ L 153, 22.5.2014, p. 62–106.

recommends specifying in the operational part of the Proposal all the aspects related to the creation of synergies on both standardisation and certification on cybersecurity as well as synergies between this Proposal and the Union data protection law in the area of market surveillance and enforcement (such as structured cooperation among the relevant bodies, provisions mandating information sharing, including personal data, in specific cases, etc.).

24. Furthermore, the EDPS considers it necessary to explicitly clarify that the Proposal does not seek to affect the application of existing EU laws governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments.

5. Critical digital products for the processing of personal data and European cybersecurity scheme

25. Recital 39 states that the Proposal aims to create synergies with Regulation (EU) 2019/881 on the EU Cybersecurity Act[17] that establishes a voluntary European cybersecurity certification framework for ICT products, processes and services.

26. Furthermore, in line with Article 6(5)(b) of the Proposal, the Commission is empowered to adopt delegated acts in accordance to specify categories of highly critical products with digital elements for which the manufacturers should be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme. When determining such categories of highly critical products with digital elements, the Commission should take into account, inter alia, the intended use of performing critical or sensitive functions, such as processing of personal data[18].

27. In this regard, the EDPS welcomes the fact that the Proposal acknowledges that the processing of personal data is a critical and sensitive function and might as such require the corresponding critical products with digital elements to obtain a European cybersecurity certificate under a European cybersecurity certification scheme. At the same time, the EDPS recommends clarifying in in the preamble that obtaining a European cybersecurity certification under the Proposal does not guarantee compliance with the GDPR.

6. Penalties applicable to infringements by economic operators

28. In line with the Proposal, the Member States shall establish penalties applicable to infringements by economic operators, with limits set out as follows:

[17] 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 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15–69).
[18] Article 6(2)(c) of the Proposal.

- Non-compliance with essential requirements set out in Annex I and obligations for manufactures shall be subject to administrative fines of up to €15 million or up to 2.5% of its global revenue, whichever is higher.
- Non-compliance with other obligations under the CRA shall be subject to administrative fines of up to €10 million or up to 2% of global revenue, whichever is higher.

29. In case incorrect, incomplete or misleading information is supplied to notified bodies and market surveillance authorities in reply to a request, the offender shall be subjected to administrative fines of up to €5 million or up to 1% of global revenue, whichever is higher.

30. The EDPS welcomes the proposed penalties, which are similar to those of the GDPR for a breach Article 32 GDPR on the security of processing, with a maximum fine of 2.5% of global annual turnover. As a result, the Proposal could serve as yet another form of protection for individuals that reside within EU Member States, in conjunction with the provisions of the GDPR.

7. Conclusions

31. In light of the above, the EDPS makes the following recommendations:

(1) to include the data protection by design and by default principle in the essential cybersecurity requirements of products with digital elements;

(2) to explain in the preamble the importance of products with digital elements that perform cryptographic operations, including encryption at rest and in transit and pseudonymisation that are necessary for effective information security, cybersecurity, data protection and privacy;

(3) to add in Annex II tangible and intangible products with digital elements that perform cryptographic operations;

(4) to delete Regulation (EU) 2017/745 from the list of the legislations excluded from the application of the Proposal;

(5) to clarify expressly in the Proposal what are the elements of the essential requirements referred to by Article 3(3)(e) of Directive 2014/53/EU on personal data and privacy;

(6) to specify in the operational part of the Proposal the practical aspects related to the creation of synergies on both standardisation and certification on cybersecurity as well as synergies between this Proposal and the Union data protection law in the area of market surveillance and enforcement;

(7) to clarify that the Proposal does not seek to affect the application of existing EU laws governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments;

(8) to add relevant definitions of ‘free software’, ‘open source software’ and ‘free and open source software’;

(9) to clarify in recital of the Proposal that obtaining a European cybersecurity certification under the Proposal does not guarantee compliance with the GDPR.

Brussels, 9 November 2022

(e-signed)
Wojciech Rafał WIEWIÓROWSKI