EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

10 May 2021

Opinion 7/2021

on the Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) 1060/2009, (EU) 648/2012, (EU) 600/2014 and (EU) 909/2014

edps.europa.eu

The European Data Protection Supervisor (EDPS) is an independent EU authority, its responsibilities are outlined 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'. Under Article 58(3)(c) of Regulation 2018/1725, the EDPS shall have the power 'to issue on his or her own initiative or on request, opinions to Union institutions and bodies and to the public on any issue related to the protection of personal data'.

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

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 Article 58 of Regulation (EU) 2018/1725.

Executive Summary

The European Commission adopted on 24 September 2020 a Proposal for a Regulation on Digital Operational Resilience for the financial sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (the "Proposal"). The Proposal establishes a comprehensive framework on digital operational resilience for EU financial entities, based on five key areas, namely the management of ICT risks (Chapter II), the management, classification and reporting of incidents (Chapter III), digital operational resilience testing (Chapter IV), management of third-party risks and regulation of critical ICT service providers (Chapter V) and information sharing (Chapter VI).

The EDPS welcomes the objectives of the Proposal, and considers it essential for the European Union financial market's stability that financial institutions count with a sound, comprehensive and well-documented ICT risk management framework

The EDPS highlights the importance of ensuring that any processing operation in the context of the operations of the financial entities is based on one of the legal basis laid down in Article 6 of the GDPR. Moreover, the EDPS highlights the importance for financial entities of embedding within their digital operational resilience framework a strong data protection governance mechanism, which clearly identifies the roles and responsibilities of the controller and the processor, as well as the processing activities that will take place.

Regarding the international transfers to ICT third-party service providers established in a third-country, the EDPS recalls that any international transfer of personal data must comply with the requirements of Chapter V of the GDPR as interpreted in the case-law of the CJEU, including the judgment in *Schrems II*.

Regarding the sharing arrangements on intelligence and cyber threat information amongst financial entities, the EDPS highlights that the protection of personal data does not constitute an obstacle to intelligence sharing in the financial sector. Rather, data protection requirements should be perceived as a basic requirement which should be complied with to ensure the safeguard of the rights of individuals. In this context, the EDPS encourages the adoption also in the financial sector of codes of conduct in accordance with Article 40 of the GDPR, particularly in view of clearly establishing the roles of the main stakeholders in the processing of personal data, as well as ensuring a fair and transparent processing.

Regarding the publication of administrative fines, the EDPS recommends including, among the criteria for consideration of the competent authority, the risks to the protection of the personal data of the individuals. Moreover, the EDPS recalls that the principle of storage limitation requires that personal data is stored for no longer than is necessary for the purposes for which the personal data are processed.

Regarding the notification of data breaches, the EDPS highlights that the wording of Recital 42 of the Proposal is incompatible with Article 33 of the GDPR. Therefore, the EDPS recommends deleting the reference to data protection authorities from Recital 42 of the Proposal, as well as slightly amending Article 17 of the Proposal in accordance with the recommendations of this Opinion.

Table of Contents

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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 (the General Data Protection Regulation)[1],

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[2], and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1 BACKGROUND

1. The European Commission adopted on 24 September 2020 a Proposal for a Regulation on Digital Operational Resilience for the financial sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (the "**Proposal**"). The Proposal establishes a comprehensive framework on digital operational resilience for EU financial entities, based on five key areas, namely the management of ICT risks (Chapter II), the management, classification and reporting of incidents (Chapter III), digital operational resilience testing (Chapter IV), management of third-party risks and regulation of critical ICT service providers (Chapter V) and information sharing (Chapter VI).

2. This Proposal belongs to a package that includes also a proposal for a regulation to build markets in cryptoassets[3] (the "**MICA Regulation**"), a proposal on a pilot regime for Market Infrastructures based on DLT[4], and a proposal to clarify or amend certain related EU financial services rules[5]. The EDPS was consulted on the Proposal on the pilot regime for Market Infrastructures based on DLT and delivered his Opinion on 23 April 2021[6]. He was also consulted on the MICA Regulation on 29 April 2021 and will deliver his opinion in line with Article 42(1) of Regulation (UE) 2018/1725.

3. On 15 March 2021, the European Commission requested the European Data Protection Supervisor (the "EDPS") to issue an opinion on the Proposal, in accordance with Article 42(1) of Regulation (UE) 2018/1725. These comments are limited to the provisions of the Proposal that are relevant from a data protection perspective.

2 GENERAL COMMENTS

4. The EDPS notes that the Proposal aims, *inter alia*, at consolidating and upgrading the ICT risk requirements addressed so far separately in different legislation[7], as well as laying down rules to complete the ICT-related incident reporting regime in the financial sector legislation and

remove any existing overlaps and duplications8. Moreover, it lays down rules to enable coordinated testing by financial entities and competent authorities, thus facilitating the mutual recognition across Member States of advanced testing for significant financial entities[9]. Furthermore, the Proposal establishes certain key principles to guide financial entities' management of ICT third-party risk, accompanied by a set of core contractual rights to ensure certain minimum safeguards[10]. Finally, the Proposal aims at setting up a framework to facilitate the sharing of cyber threat information and intelligence amongst financial entities.

5. **The EDPS welcomes the objectives of the Proposal, and considers it essential for the European Union financial market's stability that financial institutions are to implement a sound, comprehensive and well-documented ICT risk management framework** to address their own ICT risks and manage ICT third-party risks, including appropriate contractual arrangements for the use of ICT services. Moreover, the EDPS acknowledges the importance of establishing clear rules as to the ICT-related incident management process, as well as with regard to the scope and boundaries of information sharing on cyber threats and intelligence among financial entities[11].

6. The EDPS notes that Recital 32 of the Proposal provides that mechanisms for voluntary information sharing arrangements should be conducted in full compliance with the applicable competition law rules of the Union *"as well as in a way that guarantees the **full respect of Union data protection rules** mainly Regulation (EU) 2016/679 of the European Parliament and of the Council, in particular in the context of the processing of personal data that is necessary **for the purposes of the legitimate interest** pursued by the controller or by a third party, as referred to in point (f) of Article 6(1) of that Regulation*". In this regard, we recall that pursuant to Article 6(1)(f) GDPR processing shall be lawful if it "*is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*".In this context, we draw attention to the Article 29 WP Opinion 06/2014 on the notion of legitimate interests of the data controller[12], which clarifies that this legal basis requires a balancing of the legitimate interests of the controller, or any third parties to whom the data are disclosed, against the interests or fundamental rights of the data subject. The outcome of this balancing test will determine whether this legal basis may be relied upon as a legal ground for processing. At the same time, the EDPS highlights that the current wording of Recital 32 of the Proposal may lead to confusion as it appears to point to the sole legal basis from Article 6(1) GDPR to be relied upon, whereas the EDPS considers that Article 6(1)(c) or (e) should not be excluded as possible legal bases in certain cases. Therefore, the EDPS suggests deleting the last part of sentence in Recital 32 of the Proposal, referring specifically to Article 6(1)(f) of the GDPR.

7. Moreover, the EDPS highlights the importance for financial entities of embedding within their digital operational resilience framework a **strong data protection governance mechanism**, which clearly identifies the roles and responsibilities of the controller and the processor, as well as the processing activities that will take place. Only this way financial entities will guarantee the rights of data subjects in accordance with the GDPR, and ensure compliance with their obligations regarding the security of personal data (i.e. implementation of appropriate security technical and organisational measures, notification of personal data breaches to the supervisory authority and to the data subjects in due time, carry out of data protection impact assessments where relevant, etc.).

3 SPECIFIC COMMENTS

3.1 Regarding the international transfers to ICT third-party service providers established in a third-country

8. The EDPS welcomes that Article 26(2) of the Proposal regarding the preliminary assessment of ICT concentration risk and further sub-outsourcing arrangements requires that where contractual arrangements for the use of ICT services are concluded with an ICT third-party service provider established **in a third-country**, financial entities shall consider a number of factors, including in particular **the respect of data protection.** In this regard, the EDPS recalls that any international transfer of personal data must in any event comply with the requirements of Chapter V of the GDPR, as interpreted in the case-law of the CJEU, including the judgment in *Schrems II*[13].

9. The EDPS recalls that pursuant to Article 45(1) of the GDPR, a transfer of personal data to a third country may take place where the Commission has decided that the third country ensures an adequate level of protection (the adequacy decision). In the absence of an adequacy decision, financial entities aiming at outsourcing services or using IT infrastructure involving a transfer of personal data would need to perform their assessment on the security of the transfer, and may take recourse to **Standard Contractual Clauses**, as this would seem the most relevant transfer tool. In this regard, the EDPS draws attention to the EDPB - EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on Standard Contractual Clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679[14].

10. The EDPS welcomes that the Proposal specifically mentions the protection of personal data as one of the essential areas to which the contractual arrangements on the use of ICT services need to make reference. In particular, Article 27(2)(c) of the Proposal states that "*The contractual arrangements on the use of ICT services shall include provisions on accessibility, availability, integrity, security* ***and protection of personal data*** *and on ensuring access, recovery and return [...]*".

3.2 Regarding the information sharing arrangements

11. The EDPS notes that in relation to intelligence sharing between financial entities on ICT threats the Proposal states, that "*in the absence of guidance at Union level,* ***several factors seem to have inhibited such intelligence sharing****, notably uncertainty over the compatibility with the data protection, anti-trust and liability rules*". In this regard, the EDPS highlights that **the protection of personal data does not constitute an obstacle to intelligence sharing** in the financial sector. Rather, data protection requirements should be perceived as a basic requirement, which should be complied with to ensure the safeguard of the rights of individuals within the digital operational resilience framework of financial entities. Moreover, the EDPS recalls the important role of national DPAs in promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to processing[15], as well as the awareness of controllers and processors of their obligations under the GDPR[16]. Moreover, the EDPS draws attention to the European Data Protection Board's guidance provided in its guidelines, recommendations and best practices to encourage consistent application of the GDPR[17].

12. The EDPS welcomes that the Proposal subjects the exchange of cyber threat information and intelligence amongst financial entities to the requirement that such sharing "is implemented through information-sharing arrangements that protect the *potentially sensitive nature of the*

information shared, and that are ***governed by rules of conduct in full respect of business confidentiality, protection of personal data*** *and guidelines on competition policy*"[18]. In this regard, **the EDPS encourages the adoption also in the financial sector of codes of conduct in accordance with Article 40 of the GDPR**, particularly in view of clearly establishing the roles of the main stakeholders in the processing of personal data, as well as ensuring a fair and transparent processing.

3.3 Regarding the publication of administrative fines

13. The EDPS notes that Article 48(3) of the Proposal allows competent authorities to adopt, in certain cases, **alternative measures to the publication of the identity and personal data** of the natural and legal persons on which it imposes an administrative sanction, including to defer its publication until the moment where all reasons for non-publication cease to exist, to **publish it on an anonymous basis,** in accordance with national law or refrain from publishing it, where the aforesaid two options are deemed either insufficient to guarantee a lack of any danger for the stability of financial markets, or where such a publication would not be proportional with the leniency of the imposed sanction[19]. These alternative measures may be taken in the cases where the competent authority, following a case-by-case assessment, considers that the publication would be disproportionate, would jeopardise the stability of financial markets or the pursuit of an on-going criminal investigation, or would cause, insofar as these can be determined, disproportionate damages to the person involved. **The EDPS recommends including, among the criteria for consideration of the competent authority, the risks to the protection of the personal data of the individuals.**

14. The EDPS notes that Article 48(6) of the Proposal establishes that competent authorities shall ensure that any publication of administrative fines "*remain on their official website for at least* ***five years*** *after its publication.* ***Personal data*** *contained in the publication* ***shall only be kept*** *on the official website of the competent authority* ***for the period which is necessary in accordance with the applicable data protection rules***". The EDPS recalls that the principle of storage limitation requires that personal data is stored for no longer than is necessary for the purposes for which the personal data are processed. Therefore, financial entities should adopt measures to ensure that the information on the administrative fines is deleted from their website after the five years have elapsed, or earlier, if it is no longer necessary.

3.4 Regarding the notification of data breaches

15. Pursuant to Recital 42 of the Proposal "*Direct reporting would enable financial supervisors' access to information on ICT-related incidents. Nevertheless,* ***financial supervisors should pass on this information to non-financial public authorities*** *(NIS competent authorities, national data protection authorities and law enforcement authorities for incidents of criminal nature)*". Moreover, Article 17 of the Proposal requires that financial entities report major ICT-related incidents to the relevant competent authority as referred to in Article 41 of the Proposal, and within the time-limits laid down in paragraph 3 thereof.

16. Importantly, the EDPS highlights that the wording of **Recital 42 of the Proposal is incompatible with Article 33 of the GDPR**, which imposes a direct obligation on the controller, in case of a data breach, to notify without undue delay and not later than 72 hours after having become aware of a data breach, to the relevant data protection supervisory authority. Therefore, the EDPS recommends deleting the reference to data protection authorities from Recital 42 of the Proposal, as well as including the following wording in Article 17 of the Proposal: "*Where the major ICT-related indent is also a case of a personal data breach,*

financial entities shall notify it to the relevant data protection authority and to the affected data subject(s), where relevant, in line with art. 33 of the GDPR".

17. Nevertheless, the EDPS agrees that different kind of notifications required by different EU acts may contain very similar information. Thus, he considers that the idea of a Hub, as mentioned in Recital 43, is in longer term inevitable. The EDPS is ready to discuss such possibility, as well as involve other GDPR supervisory authorities in such discussion which should not be only limited to ESA, ECB and ENISA.

18. Moreover, the EDPS highlights that the term "*information leakage*" used in Article 8(3)(c) of the Proposal is not defined. In order to avoid confusion, the EDPS recommends substituting such term by "ICT breach" or "breach of confidentiality", as both terms are already used in the Proposal.

19. The EDPS notes that Article 23(2) of the Proposal requires that "*threat led penetration testing shall cover at least the critical functions and services of a financial entity, and shall be performed on live production systems supporting such functions*". The EDPS considers that testing, product development or research of the ICT systems should not be carried out on live production systems containing personal data of customers[20]. Therefore, the EDPS recommends amending the aforesaid requirements as follows "(...) *shall be performed on live production systems supporting such functions only when the systems do not contain personal data"* (emphasis added).

4 CONCLUSIONS

In light of the above, the EDPS:

- Highlights the importance of ensuring that **any processing operation** in the context of the operations of the financial entities **is based on one of the legal basis of Article 6 of the GDPR**, and indicates Article 6(1)(c), (e) and (f) of the GDPR as possible legal basis for consideration by financial entities.
- The EDPS highlights the importance for financial entities of embedding within their digital operational resilience framework a **strong data protection governance mechanism**, which clearly identifies the roles and responsibilities of the controller and the processor, as well as the processing activities that will take place.
- The EDPS recalls that **any international transfer of personal data by financial entities** to a ICT third-party service provider established in a third-country **must comply with the requirements of Chapter V of the GDPR**, and where carried out, be subject to appropriate safeguards in line with the data protection framework and the case-law of the CJEU, in particular the Schrems II case. Such financial entities may take recourse to the Standard Contractual Clauses, as it would seem as the most relevant transfer tool.
- The EDPS highlights that the **protection of personal data does not constitute an obstacle to intelligence sharing in the financial sector**. Rather, data protection requirements should be perceived as a basic requirement to be complied with to ensure the safeguard of the rights of individuals within the digital operational resilience framework of financial entities.
- The EDPS **encourages the adoption also in the financial sector of codes of conduct** in accordance with Article 40 of the GDPR, particularly in view of clearly establishing the roles of the main stakeholders in the processing of personal data, as well as ensuring a fair and transparent processing.

- Regarding the **publication of administrative sanctions**, the EDPS recommends including, among the criteria for consideration of the competent authority, **the risks to the protection of personal data of the individuals**.
- In accordance with the principle of storage limitation, the EDPS recommends financial entities to adopt measures to ensure that the **information on the administrative fines are deleted from their website after the five years have elapsed, or before** if, it is no longer necessary.
- The EDPS highlights that the **wording of Recital 42 of the Proposal is incompatible with Article 33 of the GDPR**. The EDPS hence recommends deleting the reference to data protection authorities from Recital 42 of the Proposal, as well as amending Article 17 of the Proposal to include a reference to the obligation of notification of data breaches to the relevant data protection authorities.
- The EDPS recommends amending Article 23(2) of the Proposal to ensure that testing, product development or research of the ICT systems may not be carried out on live production systems containing personal data of customers.

Brussels, 10 May 2021

Wojciech Rafał WIEWIÓROWSKI

(e-signed)

Notes

[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 (General Data Protection Regulation), L119 of 4.5.2016*

[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, L 295, 21.11.2018*

[3] *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final. Available at EUR-Lex - 52020PC0593 - EN - EUR-Lex (europa.eu)*

[4] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a pilot regime for market infrastructures based on distributed ledger technology*

COM/2020/594 final, available at EUR-Lex - 52020PC0594 - EN - EUR-Lex (europa.eu)

[5] *Proposal for a Directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341, COM/2020/596 final. Available at EUR-Lex - 52020PC0596 - EN - EUR-Lex (europa.eu)*

[6] *Opinion 6/2021 on the Proposal for a Pilot Regime for Market Infrastructures based on Distributed Ledger Technology, available at 2021-0219_d0912_opinion_6_2021_en_0.pdf (europa.eu)*

[7] *Recital 12*

[8] *Recital 22*

[9] *Recital 24*

[10] *Recital 27*

[11] *In this regard, see more broadly the EDPS Guidelines on the protection of personal data in IT governance and IT management of EU institutions, as possible guidance, mutatis mutandis, also in this case.*

The Guidelines are available at:

it_governance_management_en.pdf (europa.eu)

[12] *Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf*

[13] *Judgment of 16 July 2020, case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*

[14] *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf*

[15] *Article 57(1)(b) of the GDPR*

[16] *Article 57(1)(d) of the GDPR*

[17] *Article 70(1)(e) of the GDPR*

[18] *Article 40(1)(b) of the Proposal*

[19] *Article 48(3) of the Proposal*

[20] *See in this regard, the EDPS Guidelines on the protection of personal data in IT governance and IT management of EU institutions, paragraph 80, 81, 82, available at https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf stating that:*

80. In the testing phase, sampling of real personal data should be avoided, as such data cannot be used for purposes for which it was not collected and using it in testing environments may result in making personal data available to unauthorised individuals.

81. Where possible, artificially created test data should be used, or test data which is derived from real data so that its structure is preserved but no actual personal data is contained in it. Different such techniques have been applied successfully .

82. Where thorough and cautious analysis shows that generated test data cannot provide sufficient assurance for the validity of the tests, a comprehensive decision must be taken and documented, which defines which real data shall be used in the test, as limited as possible, the additional technical and organisational safeguards which are established in the testing environment. Special categories of data can only be used in real data testing with the explicit consent of the individuals concerned.