C/2026/2621

26.5.2026

OPINION OF THE EUROPEAN CENTRAL BANK

of 10 March 2026

on a proposed regulation as regards the simplification of the digital legislative framework (Digital Omnibus)

(CON/2026/9)

(C/2026/2621)

Introduction and legal basis

On 9 December 2025 the European Central Bank (ECB) received a request from the European Parliament for an opinion on a proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) [1] (hereinafter the 'proposed regulation').

The ECB's competence to deliver an opinion is based on Articles 127(4) and 282(5) of the Treaty on the Functioning of the European Union since the proposed regulation contains provisions falling within the ECB's fields of competence, including, in particular, the implementation of monetary policy pursuant to Article 127(2), first indent, and Article 282(1) of the Treaty, the smooth operation of payment systems pursuant to Article 127(2), fourth indent, and Article 282(1) of the Treaty, the prudential supervision of credit institutions pursuant to Article 127(6) of the Treaty, and the ECB's tasks relating to the collection of statistical information pursuant to Article 5 of the Statute of the European System of Central Banks and of the European Central Bank (hereinafter the 'Statute of the ESCB'). In accordance with Article 17.5, first sentence, of the Rules of Procedure of the European Central Bank, the Governing Council has adopted this opinion.

1. General observations

1.1. The ECB supports the proposed regulation, which is an important reform aiming to simplify and optimise the application of the digital rulebook in the Union. To the extent that the proposed regulation is effective in delivering on its objectives of promoting policies that strengthen the Union's competitiveness, and lightening the regulatory load for people, businesses and administrations, it will remove impediments to the provision of services and support the development of the digital economy in the Union, whilst taking into account the need to maintain the highest standards in promoting the Union's values, including upholding fundamental rights. The digital economy is increasing in importance and may have implications for the conduct of monetary policy as it affects the environment in which monetary policy operates by transforming patterns of consumption and production, business models and relative prices heterogeneously across the euro area and the Member States. These developments have important effects on monetary-policy relevant variables and their measurement, including employment, productivity, potential output and inflation. They also affect the way in which monetary policy decisions are transmitted to households and firms, adding to the uncertainty and complexity faced by policymakers.

1.2. In particular, the ECB welcomes the proposals to simplify the arrangements for government-to-business and business-to-government data sharing and provisions governing the processing of personal data in Regulation (EU) 2023/2854 of the European Parliament and of the Council [2] (hereinafter the 'Data Act'). The ECB is extensively involved in the collection, development, production and dissemination of data, which it uses to undertake the tasks and activities falling within its fields of competence. This competence includes the collection of statistical information, where necessary, to undertake the tasks of the European System of Central Banks (ESCB) under Article 5 of the Statute of the ESCB. The ECB is also involved in many cooperative initiatives supporting data sharing and collaboration with other Union institutions, bodies, offices and agencies, as well as with the competent authorities of the Member States, third countries and international organisations. When undertaking its tasks, it

[1] COM (2025) 837 final.

[2] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), (OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

may also process personal data in certain circumstances in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council ([3]) (hereinafter the 'EUDPR'). For these reasons, the ECB supports measures that will build a coherent and cohesive regulatory framework to support the availability and use of data.

1.3. The ECB is also responsible for ensuring compliance with Regulation (EU) 2022/2554 of the European Parliament and of the Council ([4]) (hereinafter 'DORA') for credit institutions classified as significant pursuant to Article 6(4) of Council Regulation (EU) No 1024/2013 ([5]) in accordance with the prudential supervisory powers and tasks conferred by that Regulation ([6]). In this capacity, the ECB receives reports from significant credit institutions to their national competent authorities concerning major information and communications technology-related incidents (hereinafter 'ICT-related incidents') and significant cyber threats. In addition, one of the basic tasks of the ESCB is to promote the smooth operation of payment systems, pursuant to Article 127(2) of the Treaty, fourth indent, as mirrored in Article 3.1 of the Statute of the ESCB. In this context, the ECB receives incident reports from payment institutions and electronic money institutions, as well as from credit institutions, pursuant to DORA. In view of these responsibilities and tasks, the ECB generally welcomes efforts to further simplify and harmonise the ICT-related incident reporting framework within the Union and implement centralised reporting of major ICT-related incidents. As the financial sector has been at the forefront of implementing a harmonised, comprehensive and effective framework for incident reporting, the ECB supports measures that simplify compliance with incident-reporting requirements, based on the experience gained in the financial sector.

1.4. However, the ECB has concerns regarding the extent to which the proposed regulation would give effect to the objective of simplification in specific cases where it does not alleviate the burden of regulatory compliance faced by businesses and public authorities. Accordingly, the ECB offers in this Opinion some specific technical observations and suggestions on the proposed regulation.

1.5. Because of these concerns, the ECB also welcomes that the Commission will conduct an evaluation of the main chapters of the Data Act by 12 September 2028 and of the new chapters within five years of the entry into force of the proposed regulation ([7]). Likewise, it is important that the review clause in DORA ([8]) remains unchanged, requiring the Commission to carry out a review and submit a report on the functioning of many aspects of DORA. This review process should ensure that the regulations concerned continue to function effectively to serve their objectives, thereby supporting the development of the digital economy in the Union.

2. **Digital rules**

2.1. The ECB fully supports the proposed regulation as a first step to simplify the digital rulebook and optimise its application. The body of digital rules that has been developed over time in the fields of data, artificial intelligence, online platforms, data protection and cybersecurity has become complex, and now contains fragmented and overlapping provisions which create uncertainty for public authorities and businesses alike.

([3]) 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 L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([4]) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([5]) Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63, ELI: http://data.europa.eu/eli/reg/2013/1024/oj).

([6]) Article 46, point (a), of DORA.

([7]) Article 1(26) of the proposed regulation amending Article 49 of the Data Act. See also paragraph 1.2 of Opinion CON/2022/30 of the European Central Bank of 5 September 2022 on a proposal for a regulation on harmonised rules on fair access to and use of data (Data Act) (OJ C 402, 19.10.2022, p. 5).

([8]) Article 58 of DORA.

2.2. The consolidation in the Data Act of rules in Regulation (EU) 2022/868 of the European Parliament and of the Council ([9]) on the re-use of protected data held by public sector bodies in the Member States with the rules in Directive (EU) 2019/1024 of the European Parliament and of the Council ([10]) on the re-use of documents held by public sector bodies of the Member States or public undertakings establishes a more coherent structure and more consistent definitions of key terms, making it easier to apply data sharing rules. This is supported by the repeal of outdated rules, especially those in Regulation (EU) 2018/1807 of the European Parliament and of the Council ([11]).

2.3. For national central banks (NCBs), which are commonly public sector bodies of the Member States and therefore subject to rules seeking to facilitate the re-use of data, this provides welcome clarity. The ECB and NCBs will also benefit from clearer arrangements concerning the availability of data, in particular, sources of open data which have been classified as high-value datasets ([12]). These datasets are used extensively by the ECB when performing its task under Article 5(1) of the Statute of the ESCB to collect statistical information that is necessary to undertake the tasks of the ESCB.

2.4. For example, information on companies and company ownership is used to maintain the Register of Institutions and Affiliates (RIAD), which is a shared dataset of reference data on legal and other statistical institutions, the collection of which supports business processes across the Eurosystem and the performance of the tasks of the ESCB and the Single Supervisory Mechanism (SSM) ([13]). Where the ECB can rely on open data, i.e. data in an open format that can be freely used, re-used and shared by anyone for any purpose ([14]), it is able to reduce the burden of reporting such data by reporting agents and to share this information without restriction within the ESCB and with other public authorities with which it cooperates. The ECB welcomes that the arrangements concerning the availability of data and documents from government to businesses ([15]) are without prejudice to the Union's legal regime excluding access to sensitive data and documents on grounds of statistical confidentiality and professional secrecy.

2.5. The proposed regulation introduces an important amendment ([16]) of the obligation for data holders to make data available to the ECB – as well as other public sector bodies, the Commission and Union bodies – where there is an exceptional need to use that data ([17]). This provision allows the ECB to request data holders to make data available, where necessary, to respond to a public emergency or where an exceptional need is demonstrated. As data holders are defined broadly ([18]), the provision allows the ECB to collect data in these exceptional cases from a wider range of persons than is permitted when the ECB collects statistical information on the basis of its existing powers. The

([9]) Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

([10]) Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (OJ L 172, 26.6.2019, p. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj).

([11]) Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (OJ L 303, 28.11.2018, p. 59, ELI: http://data.europa.eu/eli/reg/2018/1807/oj).

([12]) Under Article 13(1) of the Open Data Directive the thematic categories of high-value datasets are geospatial, earth observation and environment, meteorological, statistics, companies and company ownership and mobility. Under Article 13(2), the Commission is empowered to adopt delegated acts in order to amend Annex I by adding new thematic categories of high-value datasets in order to reflect technological and market developments.

([13]) Guideline (EU) 2018/876 of the European Central Bank of 1 June 2018 on the Register of Institutions and Affiliates Data (ECB/2018/16) (OJ L 154, 18.6.2018, p. 3, ELI: http://data.europa.eu/eli/guideline/2018/876/oj).

([14]) See recital 16 of Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (OJ L 172, 26.6.2019, p. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj).

([15]) Article 1(18) of the proposed regulation, inserting a new Chapter VIIc into the Data Act.

([16]) Article 1(7) of the proposed regulation, inserting a new Article 15a into the Data Act.

([17]) Articles 14 and 15 of the Data Act.

([18]) 'Data holder' is defined in Article 2(13) of the Data Act as 'a natural or legal person that has the right or obligation, in accordance with the Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service'.

ECB may only collect statistical information from members of the reporting population defined by Council Regulation (EC) No 2533/98 ([19]), which primarily fall within the 'financial corporations' sector as defined in the European system of accounts ([20]) or are legal and natural persons which hold certain financial positions or engage in financial transactions.

2.6. As the ECB has previously opined, there are considerable benefits to allowing public authorities to access and use data from private data holders for defined public interest purposes ([21]). When performing its monetary policy task, the ECB makes extensive use not only of official statistics produced by the ECB, with the assistance of NCBs and the European Statistical System (ESS), but also of non-official and non-traditional data sources. Non-traditional data may be sourced, for example, from high frequency price information, population mobility indicators or other sources of data which are not necessarily held by financial corporations. The ECB only has the power to request this data from private data holders in cases where there is an exceptional need.

2.7. The main change that the proposed regulation would introduce is to limit the cases in which this power can be exercised to public emergencies, excluding other cases in which there may be an exceptional need to use data. The ECB would need to demonstrate an exceptional need to use certain data to carry out its statutory duties in the public interest when responding to, mitigating or supporting the recovery from a public emergency.

2.8. The ECB supports the objectives of these changes, considering it appropriate to simplify the business-to-government sharing framework under the Data Act and to clarify any ambiguities that may have arisen in the imposition of obligations on businesses. It also supports the view that it is essential to preserve the role of official statistics under the Data Act, as the updated Union framework on European statistics under Regulation (EC) No 223/2009 of the European Parliament and of the Council ([22]) does not address public emergencies ([23]).

2.9. However, unlike the members of the ESS, who may collect data from private data holders under certain conditions to perform their statistical tasks ([24]), the ECB does not have any powers to collect statistical information from private data holders which are not reporting agents, apart from cases where there is an exceptional need. The ECB may only rely on mechanisms that allow for data sharing from the ESS to the ESCB to source such data. If the scope of the relevant provision is narrowed to cover only a public emergency, it is extremely important to ensure that it may be applied smoothly and without ambiguity in situations of urgency in which additional sources of data are needed for the ECB to perform either its statistical collection task or other central banking or prudential supervisory tasks. The ECB therefore recommends further simplifying the conditions which must be fulfilled by public authorities to request data, as this would also serve to minimise the complexities that data holders face when verifying whether these conditions are met.

2.10. In addition, the ECB considers that further steps should be taken to clarify the definition of a 'public emergency'. One element of the definition is that it must be 'determined or officially declared in accordance with the relevant procedures under Union or national law' ([25]). But as there is a fragmented set of legal bases in primary and secondary law on which the determination or declaration of a public emergency may be made, it should be clearer that where such a determination or declaration is made, the definition of a 'public emergency' does not require any

([19]) Article 2 of Council Regulation (EC) No 2533/98 of 23 November 1998 concerning the collection of statistical information by the European Central Bank (OJ L 318, 27.11.1998, p. 8, ELI: http://data.europa.eu/eli/reg/1998/2533/oj).

([20]) See the European System of National and Regional Accounts (ESA 2010) available on Eurostat's website at www.ec.europa.eu/eurostat.

([21]) Paragraph 2.3.1 of Opinion CON/2022/30.

([22]) Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164, ELI: http://data.europa.eu/eli/reg/2009/223/oj).

([23]) Recital 15 of the proposed regulation.

([24]) Article 17b of Regulation (EC) 223/2009.

([25]) Article 2(29) of Regulation (EU) 2023/2854.

additional criteria to be met – in view of the urgency with which a public emergency needs to be addressed. By way of example, Regulation (EU) 2024/2747 of the European Parliament and of the Council ([26]) allows the Council to activate an internal market vigilance mode when there is a threat of a crisis that has the potential to escalate into an internal market emergency within the following six months. It should be clearer that where the tasks of the public authority include mitigating the public emergency, the threat of a public emergency should justify the exceptional need to request data. Moreover, Council Decision 2014/415/EU ([27]) establishing the Integrated Political Crisis Response arrangements for implementation of the solidarity clause (Article 222 of the Treaty) does not confine the scope of the circumstances in which the Decision applies to exceptional situations 'limited in time' ([28]). It should therefore be clearer that the definition of public emergency fully aligns with, and is not more restrictive than, the situations in which emergency arrangements are invoked under Union and national law.

2.11. With respect to the arrangements for compensation ([29]), the ECB welcomes the requirement to make data available to respond to a public emergency free of charge, except where the data holder is a microenterprise or small enterprise. However, it considers it important to ensure that when public authorities are granted access to privately held data, they should not incur unreasonable costs. As each request for data serves the public interest, data should be made available at cost and without the imposition of a 'reasonable margin' ([30]).

3. **Data protection**

3.1. The ECB welcomes the amendments in the proposed regulation which aim to simplify data protection legislation. Within the ECB's fields of competence, there are several points that merit further consideration in order to achieve the objective of simplification, both in terms of reducing the administrative burden, as well as ensuring effective, timely and secure incident reporting.

3.2. The ECB carries out a wide range of personal data processing operations in cooperation with the NCBs. Additionally, the ECB cooperates with national competent authorities (NCAs) to conduct personal data processing activities in the field of banking supervision. As a Union institution, the ECB processes personal data in accordance with the EUDPR, whereas the NCBs and NCAs process personal data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council ([31]) (hereinafter the 'GDPR').

3.3. In cases where the ECB and the NCBs and/or NCAs jointly determine the purposes and means of the processing of personal data, such processing is conducted by them as joint controllers ([32]). Conversely, where one entity determines the purposes and means of the processing and the other processes personal data on its behalf, their relationship is that of controller and processor ([33]). In both cases, the ECB processes personal data under the EUDPR, while the NCBs and NCAs process personal data under the GDPR. As a consequence, the same processing operation is simultaneously governed by two distinct, yet complementary, Union legal instruments.

([26]) Regulation (EU) 2024/2747 of the European Parliament and of the Council of 9 October 2024 establishing a framework of measures related to an internal market emergency and to the resilience of the internal market and amending Council Regulation (EC) No 2679/98 (Internal Market Emergency and Resilience Act) (OJ L, 2024/2747, 8.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2747/oj).

([27]) Council Decision 2014/415/EU of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause (OJ L 192, 1.7.2014, p. 53, ELI: http://data.europa.eu/eli/dec/2014/415/oj).

([28]) Article 2(29) of Regulation (EU) 2023/2854.

([29]) Article 1(12) of the proposed regulation, replacing Article 20 of the Data Act.

([30]) See paragraph 2.3.3 of Opinion CON/2022/30.

([31]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([32]) Within the meaning of Article 26 of the GDPR and Article 28 of the EUDPR.

([33]) Within the meaning of Article 28 of the GDPR and Article 29 of the EUDPR.

3.4. One such example is where both the ECB and those NCBs participating in TARGET Instant Payment Settlements (TIPS) process personal data within the TIPS system. In this case a joint controllership arrangement has been concluded. Similarly, the processing of personal data in the context of the future digital euro may require the conclusion of a data protection contract or arrangement between the ECB and euro area NCBs.

3.5. When performing the tasks of the ESCB and SSM in cooperation with NCBs and NCAs, it is of paramount importance for the ECB that the legal acts governing the processing of personal data are, to the greatest extent possible, aligned and mutually compatible. The ECB therefore welcomes the fact that the proposed amendments to the GDPR and to the EUDPR are being advanced in parallel, thereby contributing to the establishment of a coherent and consistent legal framework. This ensures that divergent timelines for the entry into force and application of the legal acts do not give rise to legal uncertainty.

3.6. Therefore, in light of the ECB's cooperation with NCBs and NCAs in the processing of personal data where necessary to perform the tasks of the ESCB and the SSM, the ECB shares the following points for consideration:

3.7. With regard to the single-entry point mechanism, the ECB recommends empowering joint controllers to notify personal data breaches on behalf of all the joint controllers ([34]). This is possible because the proposed regulation introduces a harmonised single-entry point through which entities may, by means of a single notification, simultaneously comply with their incident reporting obligations arising under multiple Union legal acts. By operationalising the 'report once, share many' principle, the single-entry point is intended to reduce the administrative burden on entities, whilst ensuring effective, timely and secure incident reporting. To that end, the single-entry point is intended to serve as a common channel for the submission of notifications pursuant to several legal instruments ([35]). As the ECB has previously opined, it strongly supports information-sharing among authorities to enable cross-sectoral learning, contribute to the prevention and effective management of cyberattacks, and promote the consistent assessment of ICT-related risks across the Union ([36]). Against this background, the ECB supports the introduction of the single-entry point in the context of reporting personal data breaches.

3.8. When applying the single-entry point mechanism to joint processing activities carried out by the ECB in cooperation with NCBs (and NCAs), the NCBs would benefit under the proposed regulation from the use of the single-entry point for the receipt of incident notifications. Conversely, the ECB, as a Union institution, would continue to rely under the proposed regulation on the reporting channel established by the EUDPR, whereby it notifies incidents to the European Data Protection Supervisor (EDPS) ([37]).

3.9. The ECB reiterates the need to streamline, accelerate and maximise the exchange of information on incidents, and to ensure coherence between the GDPR and the EUDPR. Thus, it would be appropriate to include the EUDPR in the Union legal acts for which the single-entry point must be used for notifications of personal data breaches.

([34]) As required by Article 34 of the EUDPR.

([35]) These include the GDPR and Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj); Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj) (eIDAS Regulation) and Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj) (CER Directive).

([36]) See paragraph 3.3.1 of Opinion CON/2022/14 of the European Central Bank of 11 April 2022 on the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (OJ C 233, 16.6.2022, p. 22).

([37]) As required by Article 34 of the EUDPR.

3.10. On the single reporting of data breaches in cases of joint controllership, the ECB maintains that joint controllers should be free to determine whether they make use of that possibility and under which conditions. The EDPS has recently confirmed that, for the purposes of determining whether the ECB is required to notify the EDPS of a personal data breach, it is irrelevant whether the ECB, as a joint controller, is responsible for the occurrence of that breach. The mere fact that the ECB is a joint controller for the processing operation in the context of which the personal data breach has occurred is sufficient to trigger its obligation to notify the EDPS, where the relevant conditions under the EUDPR are met ([38]).

3.11. It is important to note that, in the many instances where a joint controllership arrangement between the ECB and all Eurosystem NCBs is in place, a single personal data breach could give rise to up to 22 notifications, which would in all likelihood be similar or identical in content. Such a system would prove contrary to the objective of simplifying the administrative burden for public authorities. It would, therefore, be appropriate to provide that joint controllers may notify personal data breaches via the single-entry point only once to the competent supervisory authorities. In line with the simplification objectives, such a reporting system would not apply when the personal data breach in question is unlikely to result in a risk to the rights and freedoms of natural persons ([39]).

3.12. For these reasons, the ECB recommends that it should be left to joint controllers to determine whether they wish to make use of the possibility of submitting one notification on behalf of all the joint controllers in a specific joint-controllership arrangement, and under which conditions. Such notification would be submitted once via the single-entry point, and thereby be addressed to all the relevant supervisory authorities, without compromising the role that obligations to notify have in ensuring full transparency and comprehensive information exchange.

4. **Incident reporting**

4.1. As noted in paragraph 1.3, the ECB welcomes the initiative to simplify and harmonise the ICT-related incident reporting procedures and implement a centralised reporting of major ICT-related incidents. However, this should, in each case, reduce the administrative burden for supervised credit institutions, payment institutions, electronic money institutions and public authorities. In this regard, it is important to acknowledge that a certain degree of simplification of reporting procedures has already been achieved through the implementation of DORA in the financial sector. DORA effectively replaced different ICT-related incident reporting requirements for financial entities ([40]), achieving a significant reduction of the reporting burden to which they were subject and implementing effective and efficient coordination mechanisms among the different competent authorities ([41]). DORA achieved that objective by defining common taxonomies, templates and reporting procedures and with the identification of a unique entry point for these reports.

4.2. While the ECB supports these simplification efforts, it also has reservations about aspects of ICT-related incident reporting measures in the proposed regulation for three main reasons.

4.3. First, the proposal for a single-entry point is not effective in reducing the reporting burden for financial entities and other businesses which are subject to incident reporting requirements. While the single-entry point ensures that there is a single portal for incident reporting, it does not change the fact that there are still different taxonomies, templates and reporting procedures for each incident report under the different frameworks other than DORA. To report an incident, a financial entity must prepare different reports in accordance with different legislation (e.g. under the GDPR and DORA). Merely permitting these reports to be notified to one single recipient does not alleviate the administrative burden in a significant manner. For this reason, it would be appropriate to take due

([38]) EDPS Supervisory Opinion 18/2025 on a draft joint controllership arrangement between the European Central Bank and National Competent Authorities in the context of the Single Supervisory Mechanism (Case 2024-1002), available on the EDPS's website at www.edps.europa.eu.

([39]) Article 34 of the EUDPR.

([40]) See, to that effect, recitals 16, 18, 19, and 23 of DORA.

([41]) This has allowed the issue of parallel submissions under DORA, Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj) and the corresponding EBA Guidelines to be addressed, as identified in paragraph 4.2.2 of Opinion CON/2021/20 of the European Central Bank of 4 June 2021 on a proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (OJ C 343, 26.8.2021, p. 1).

account of the regulatory technical standards adopted pursuant to DORA to facilitate more efficient and streamlined reporting processes ([42]). The ECB would also welcome further alignment and, where appropriate, merging taxonomies, templates and reporting procedures for incidents under the various frameworks, with a view to achieving genuine simplification.

4.4. Second, a DORA incident report triggers time-critical processes that potentially involve the activation of crisis procedures. Including a new actor and system in the reception of these incident reports entails additional risks in terms of the availability and timely reporting of the required information. For that reason, the most effective and resilient option is for those reports to be sent directly to the competent authority as envisaged under DORA ([43]), in order to avoid any undue delay in the supervisory reaction to a potentially critical situation.

4.5. Third, the effort and expenditure already committed by the financial sector in implementing DORA, which has only applied from 17 January 2025, should be considered. Supervised credit institutions and competent authorities have invested significant resources in the implementation of the new framework. From this perspective, it would be beneficial to delay the integration of ICT-related incident reporting via the single-entry point. This would give more time to identify potential improvements and ways in which to further simplify the administrative burden for the SSM and supervised credit institutions alike.

4.6. For these reasons, the ECB proposes that DORA be excluded from the proposed regulation. It would be appropriate to gain experience separately with the new single-entry point (covering the other regulations, including the EUDPR) and the newly implemented DORA reporting regime, and then review how best to integrate them at a later stage.

Where the ECB recommends that the proposed regulation is amended, specific drafting proposals are set out in a separate technical working document accompanied by an explanatory text to this effect. The technical working document is available in English on EUR-Lex.

Done at Frankfurt am Main, 10 March 2026.

The President of the ECB
Christine LAGARDE

([42]) As envisaged in recital 54 of the proposed regulation.
([43]) Article 19 of DORA.