TECHFREEDOM
LAW FOR A DYNAMIC FUTURE

Comments of

TechFreedom

Andy Jung[i] & Agneris Sampieri Ortega[ii]

In the Matter of

Call for Evidence for a European Data Union Strategy

Ares(2025)4163996

July 20, 2025

---

[i] Andy Jung is Associate Counsel of TechFreedom, a nonprofit, nonpartisan technology policy think tank. He can be reached at ajung@techfreedom.org.
[ii] Agneris Sampieri Ortega is an AI and European Regulation Intern at TechFreedom. She can be reached at asampieri@techfreedom.org.

TABLE OF CONTENTS

INTRODUCTION

One of the primary objectives of the European Data Union Strategy is "simplification:"[1] it "aim[s] to streamline existing data rules, potentially creating a simplified, clearer, and more coherent legal framework for businesses and administrations to share data more seamlessly and at scale." [2] To simplify the European Union's data regulations, the consultation contemplates "targeted adjustments … to make the instruments work together in the best way for an effective data economy," including "facilitating digital reporting in existing legislation."[3] To that end, the consultation contemplates "developing data tools to reduce administrative burden," like deploying "[d]igital infrastructures … to enable automatic compliance with reporting obligations."[4]

The Strategy also aims "to facilitate voluntary data sharing" and "stimulate data import into the EU."[5] These objectives align with the EU's overarching goal "to establish an internal market where data can flow freely."[6] Ultimately, the EU strives to become an "AI continent," competing with the United States and China in the race to "develop[] and deploy[] … AI solutions that benefit society and the economy."[7]

Data breach reporting obligations are one subset of EU data rules sorely in need of simplification and streamlining. Currently, overlapping data breach reporting obligations in the General Data Protection Regulation, Network and Information Systems Directive 2, and Cyber Resilience Act create significant operational strain for technology companies operating in Europe. During critical phases of data breach incident response, complex reporting obligations force companies to divert attention and resources away from containment and remediation to comply with overwrought legal requirements.

More generally, overlapping data breach reporting obligations undermine the EU's goal of creating a Single Market for data and, ultimately, artificial intelligence. Simplifying data breach notification rules is necessary to achieve the stated goals of the European Data Union Strategy: facilitating voluntary data sharing and stimulating data import into and across

---

[1] Call for Evidence for a European Data Union Strategy at 2, Ares(2025)4163996 (May 23, 2025) [hereinafter *Call for Evidence*].
[2] *About this initiative*, EUROPEAN COMMISSION (May 23, 2025), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14541-European-Data-Union-Strategy_en (last visited July 19, 2025).
[3] *Call for Evidence* at 2.
[4] *Id*.
[5] *Id*.
[6] *Id*. at 1.
[7] *Shaping Europe's leadership in artificial intelligence with the AI continent action plan*, EUROPEAN COMMISSION, https://commission.europa.eu/topics/eu-competitiveness/ai-continent_en (last visited July 19, 2025).

Europe. In that sense, streamlining data rules is key to transforming Europe into a proper AI continent.

I. The EU's Overlapping Data Breach Reporting Obligations

When a technology company operating in the EU suffers a data breach, it must comply with the data breach notification rules of at least three separate regulations: the General Data Protection Regulation (GDPR), the Network and Information Systems Directive 2 (NIS 2), and the Cyber Resilience Act (CRA). Each regulation specifies distinct reporting criteria, deadlines, and recipient authorities, often across varying jurisdictions. This fragmented approach undermines the EU's stated goal of "establish[ing] an internal market where data can flow freely"—and, ultimately, hampers innovation, slowing development and adoption of artificial intelligence technologies.

To illustrate the EU's sprawling and overwrought web of overlapping data breach reporting obligations, these comments discuss, as an example, a hypothetical cloud service provider operating in Europe that has suffered a data breach. For illustrative purposes, these comments presume that the cloud service provider and the data breach satisfy relevant requirements to trigger the various reporting obligations described below.

A. Data Breach Reporting Obligations Under the GDPR

A cloud service provider operating in the EU that has suffered a data breach must comply with Articles 33[8] and 34[9] of the GDPR. Under Article 33, the cloud service provider must notify the "supervisory authority" of the relevant Member State within 72 hours of "having become aware" of the breach.[10] This notification must contain "the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned," "the name and contact details of the data protection officer or other contact point where more information can be obtained," "the likely consequences of the personal data breach," and "the measures taken or proposed to be taken … to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."[11]

In addition, under Article 34, if the data breach "is likely to result in a high risk to the rights and freedoms of natural persons," the cloud service provider must "communicate the

[8] 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), art. 33, 2016 O.J. (L 119) 1.
[9] *Id*. art. 34.
[10] *Id*. art. 33(1).
[11] *Id*. (3)(a)-(d).

personal data breach to the data subject without undue delay … describ[ing] in clear and plain language the nature of the personal data breach and contain[ing] at least the information and measures referred to" above, from Article 33 of the GDPR.[12]

B. Data Breach Reporting Obligations Under NIS 2

A cloud service provider operating in the EU that has suffered a data breach must also comply with Article 23 of NIS 2.[13] First, "within 24 hours of becoming aware of" the data breach, the cloud service provider must send "an early warning" to the "computer security incident response team" (CSIRT) of the relevant Member State indicating whether the breach "is suspected of being caused by unlawful or malicious acts or could have a cross-border impact." [14] Next, within 72 hours, the cloud service provider must send "an incident notification" to the CSIRT updating the information in the early warning, as needed, and "indicat[ing] an initial assessment of the" breach, "including its severity and impact, as well as, where available, the indicators of compromise."[15] Additionally, "upon the request of a CSIRT," the cloud service provider must submit "an intermediate report on relevant status updates." [16] Lastly, "not later than one month after the submission of the incident notification," the cloud service provider must submit "a final report" including: "(i) a detailed description of the incident, including its severity and impact; (ii) the type of threat or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures; [and] (iv) where applicable, the cross-border impact of the incident."[17]

Additionally, every three months, the cloud service provider must submit to the European Union Agency for Cybersecurity (ENISA) "a summary report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses."[18] Further, "[w]here appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services."[19]

---

[12] *Id*. art. 34(1), (2).
[13] 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 Direction), art. 23, 2022 O.J. (L 333) 80.
[14] *Id*. (4)(a).
[15] *Id*. (4)(b).
[16] *Id*. (4)(c).
[17] *Id*. (4)(d).
[18] *Id*. (9).
[19] *Id*. (1).

C. Data Breach Reporting Obligations Under CRA

A cloud service provider operating in the EU that has suffered a data breach must also comply with Article 14 of CRA.[20] The cloud service provider must notify "simultaneously" the relevant CSIRT and ENISA of "any actively exploited vulnerability contained in [its] product[s] with digital elements that it becomes aware of."[21] Specifically, within 24 hours, the cloud service provider must send "an early warning notification of an actively exploited vulnerability … indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available."[22] Next, within 72 hours, the cloud service provider must send "a vulnerability notification … provid[ing] general information, as available, about the product with digital elements concerned, the general nature of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be."[23] Lastly, "no later than 14 days after a corrective or mitigating measure is available," the cloud service provider must send "a final report, including at least the following: (i) a description of the vulnerability, including its severity and impact; (ii) where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability; [and] (iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability."[24]

Under CRA, the cloud service provider must also send to the relevant CSIRT and to ENISA similar reports as described above related to "any severe incident having an impact on the security of the product with digital elements that it becomes aware of."[25] Additionally, the cloud service provider must "inform the impacted users of the product with digital elements, and where appropriate all users, of th[e] vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable."[26]

---

[20] Regulation (EU) 2024/2906 of the European Parliament and of the Council of 9 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act), art. 14, 2024 O.J. (L 2906) 1.
[21] *Id*. (1).
[22] *Id*. (2)(a).
[23] *Id*. (2)(b).
[24] *Id*. (2)(c)(i)-(iii).
[25] *Id*. (3)(a)-(c).
[26] *Id*. (8).

D. Cumulative EU Data Breach Reporting Obligations

In sum, a cloud service provider operating in the EU that has suffered a data breach must comply with various overlapping reporting obligations under the GDPR, NIS 2, and CRA, including reports to multiple supervisory bodies as well as impacted users. These reports include different criteria and timelines for submission, with some timelines as short as 24 hours after becoming aware of a data breach.

The only realistic option for full compliance by a company operating in the EU is to hire a dedicated team of employees focused on data breach response. These employees likely require specialized skills and training: for example, engineers to understand the nature of the breach, lawyers to navigate the legal requirements, and public relations professionals to communicate effectively on behalf of the organization. Hiring experts in these fields is costly: most likely, the financial burden is only manageable for large businesses. Consequently, small businesses and startups face a difficult choice between allocating significant resources to data breach response or assuming the risk of imperfect compliance. Given these options, companies may reasonably forgo or limit doing business, or at least sharing or processing data, in the EU altogether—as is already the case with several US artificial intelligence firms.[27]

II. The EU Should Implement a Unified Data Breach Reporting Framework, Create a Single Digital Compliance Portal, and Mandate Coordination and Cooperation Between Supervisory Authorities

Scholars and media commentators agree: Europe needs regulatory harmonization to compete in the digital age.[28] While these regulations individually seek to address critical issues like data protection, cybersecurity, artificial intelligence, and platform accountability, their cumulative effect has resulted in overlapping obligations that create significant bureaucratic and economic burdens for regulated entities. This impact is particularly acute for small and medium-sized enterprises (SMEs), which often lack the compliance infrastructure of larger corporations.[29]

---

[27] Graham Barlow, *OpenAI's Advanced Voice mode is unavailable in the EU, and now we might know why*, TECHRADER (Oct. 3, 2024), https://www.techradar.com/computing/artificial-intelligence/openai-s-advanced-voice-is-unavailable-in-the-eu-and-now-we-might-know-why; Oona Lagercrantz, *Europe's AI Blues: US Companies Slow Deployment*, CEPA (Nov. 1, 2024), https://cepa.org/article/europes-ai-blues-us-companies-slow-deployment/.

[28] *See* Tytti Rintamäki et al., *Impact Assessment Requirements in the GDPR vs the AI Act: Overlaps, Divergence, and Implications* (May 19, 2025), https://osf.io/6qhzj_v2.

[29] *See* Mario Draghi, *The Future of European Competitiveness: Part A* at 69 (2024) ("EU regulation imposes a proportionally higher burden on SMEs and small mid-caps than on larger companies, yet the EU lacks a

According to the European Federation of Risk Management Associations, the requirement to report similar incidents to multiple authorities under different legal instruments within varying timeframes imposes a substantial administrative load.[30] These obligations divert resources from incident containment and response efforts, undermining their overall goal of enhancing digital resilience. In practice, such fragmentation results in duplicated compliance work, legal uncertainty, and elevated costs, all of which disproportionately affect innovation and competitiveness within the SME sector.

The proposals below aim to reduce the regulatory complexity of EU data breach reporting obligations while maintaining the high standards of rights protection and security that European regulation is known for. Streamlining reporting obligations through interoperability, digital tools, and cooperation between regulatory bodies will ultimately improve compliance outcomes, while encouraging entrepreneurship and innovation.

A. A Unified Reporting Framework

The EU should establish a centralized, cross-regulation reporting mechanism for cybersecurity and data incidents. This mechanism should harmonize timelines (*e.g.*, standardizing initial notification deadlines to 72 hours) and enable a single submission to satisfy multiple legal obligations across GDPR, NIS 2, and CRA, depending on the context of the incident.

B. A Single Digital Compliance Portal

The EU should consolidate risk assessments, reporting submissions, and documentation uploads under a single digital compliance portal. This portal would serve as a one-stop shop for interacting with supervisory authorities across different regulations. The portal would be particularly useful for SMEs with limited administrative capacity.

C. Coordination and Cooperation Between Supervisory Authorities

The EU should mandate coordination between supervisory authorities, like national CSIRTs and ENISA, in order to prevent contradictory guidance and duplicate audits. A permanent inter-agency working group at the EU level could support the implementation of coherent enforcement practices. Interagency cooperation would be especially useful for SMEs, which

---

framework to assess these costs. About 80% of Commission Work Programme items are relevant to SMEs but only around half of impact assessments substantially focused on these companies. The EU also lacks a commonly agreed definition of small mid-caps and readily available statistical data.").

[30] Giovanni De Gregorio & Simona Demková, *The Enforcement Dilemmas in Europe's Digital Rulebook*, TECH POLICY PRESS (May 19, 2025), https://techpolicy.press/the-enforcement-dilemmas-in-europes-digital-rulebook.

may attempt in good faith to comply with reporting obligations to certain authorities but inadvertently fail to report to others for the same breach or security event.

CONCLUSION

Simplifying and harmonizing data breach notification obligations is necessary to achieve the objectives of the European Data Union Strategy: facilitating voluntary data sharing and stimulating data import into and across Europe. Regulatory simplification is also key to the EU's overarching goal of supercharging innovation and transforming Europe into an AI continent.

The Draghi report on EU competitiveness cites "the regulatory burden on European companies" as one of the primary challenges facing the EU's Single Market.[31] Moreover, "EU regulation imposes a proportionally higher burden on SMEs and small mid-caps than on larger companies"—hampering innovative startups that are driving the development of groundbreaking artificial intelligence technologies.[32] "In 2023, 55% of SMEs flagged regulatory obstacles and administrative burden as their greatest challenge."[33] To that end, the report calls for the EU to "fully implement the announced cut by 25% of reporting obligations and commit to achieving a further reduction for SMEs up to 50%."[34]

The Draghi report notes that "[t]he stock of regulation remains large and new regulation in the EU is growing faster than in other comparable economies."[35] Companies in Europe "need to comply with the accumulation of or frequent changes to EU legislation over time, translating into overlap and inconsistencies."[36] On the other hand, the report notes that "the US ha[s] a more federal structure and fewer authorities involved in" passing and enforcing regulations.[37]

To Europe's credit, however, the EU clearly recognizes the value of a centralized approach to regulating data security and artificial intelligence, as evidenced by the European Data Union Strategy and the Apply AI Strategy. These initiatives emphasize streamlining and centralizing regulatory efforts to facilitate a Single Market for advanced technologies.

In contrast, the United States is currently retreating from a centralized approach to regulating the technology sector, with the federal government ceding authority to the states.

---

[31] *See* Mario Draghi, *The Future of European Competitiveness: Part A* at 68 (2024).
[32] *Id*. at 69.
[33] Mario Draghi, *The Future of European Competitiveness: Part B* at 321 (2024).
[34] *Part A* at 69.
[35] *Id*. at 68-69.
[36] *Id*. at 69.
[37] *Part B* at 318.

Earlier this month, Congress failed to pass a moratorium on state laws regulating artificial intelligence; meanwhile, more than half of US states have enacted laws or regulations governing AI,[38] and, this year, "all 50 states, Puerto Rico, the Virgin Islands, and Washington, D.C. have introduced legislation on this topic."[39] Unless the US changes course, domestic AI companies will soon have to grapple with a patchwork of overlapping regulations.

Consequently, the EU has a golden opportunity to close the gap with the US in terms of developing and deploying artificial intelligence technologies. By streamlining its data rules, as well as technology regulations more generally, the EU can incentivize technology companies to expand operations in Europe and encourage entrepreneurs to found cutting-edge companies in the Loire Valley or Rhine Valley—rather than Silicon Valley. Such is the power of an integrated Single Market.

Respectfully submitted,

_____/s/_____

Andy Jung
Associate Counsel
ajung@techfreedom.org

Agneris Sampieri Ortega
AI and European Regulation Intern
asampieri@techfreedom.org

TechFreedom
1500 K Street NW
Floor 2
Washington, D.C. 20005

Date: July 20, 2025

[38] *States Can Continue Regulating AI—For Now*, BROWNSTEIN (July 7, 2025), https://www.bhfs.com/insight/states-can-continue-regulating-ai-for-now/.
[39] *Artificial Intelligence 2025 Legislation*, NCSL (Apr. 24, 2025), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation.