DIGITALEUROPE

16 FEBRUARY 2026

Digital omnibus: a first step and what must come next, now

Executive summary

The digital omnibus is Europe's first attempt to move its digital rulebook from expansion towards simplification.[1] DIGITALEUROPE welcomes this shift. The proposal responds to several issues that industry has raised for years: fragmentation of the data *acquis*, uncertainty around pseudonymisation or the proliferation of incident-reporting portals. It is a necessary first step at a critical moment for Europe's competitiveness.

As it stands, however, the omnibus is still largely an administrative clean-up. The rules that will decide whether European manufacturers and service providers can build viable data-driven and AI-enabled business models are mostly left intact. Our June 2025 simplification recommendations remain valid.[2] This paper reacts to the Commission's proposal by restating the main missing elements that must be added by the Council and Parliament as a priority, and by analysing new elements that were not covered in our original asks.

On the Data Act, consolidation is helpful, but the core issues for businesses remain untouched.[3] Mandatory, horizontal data-sharing obligations risk hollowing out Europe's emerging data-driven business models, especially in manufacturing, health and energy.

To rebalance the framework, the omnibus must:

- **Make the Data Act voluntary by default**, built on sectoral codes of conduct recognised by the Commission and used where access genuinely supports innovation and safety;

[1] COM(2025) 837 final.

[2] See DIGITALEUROPE, *Executive Brief: Removing regulatory burden for a more competitive and resilient Europe*, available at https://www.digitaleurope.org/resources/executive-brief-removing-regulatory-burden-for-a-more-competitive-and-resilient-europe/. Our full detailed recommendations on data can be found at https://cdn.digitaleurope.org/uploads/2025/06/Digital-simplification-package-Data.pdf, and those on cyber can be found at https://cdn.digitaleurope.org/uploads/2025/10/071025-Digital-simplification-package-Cyber.pdf.

[3] Regulation (EU) 2023/2854.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20

- **Fully exclude platform- (PaaS) and software-as-a-service (SaaS)** from cloud-switching obligations, which are structurally incompatible with software- and platform-based models that are Europe's competitive strength; and
- **Make trade-secret safeguards more robust and effective**, clarify temporal scope and **remove duplicative data transfers provisions**.

On the GDPR, the proposal broadly gets it right. The clarified personal-data definition and the new provisions on special categories and scientific research codify long-needed interpretations that support responsible innovation without weakening protections. The GDPR remains a fit-for-purpose framework.

The real structural problem sits in **ePrivacy**.[4] Keeping a parallel consent-centred regime for terminal-equipment data, whilst expanding exceptions, recreates the failures of past reforms and introduces new inconsistencies. The only coherent solution is to **bring all terminal-equipment processing fully under the GDPR legal bases**.

On cyber, a single entry point for incident reporting is a positive step, but simplification cannot stop at the portal. The final omnibus must:

- Deliver **a genuinely single entry point**, covering NIS2, the Cyber Resilience Act (CRA), DORA, the Critical Entities Resilience (CER) Directive, eIDAS and the AI Act,[5] using the CRA single reporting platform;
- Mandate **one harmonised reporting template**, aligned with international standards, and fix fragmented reporting timelines, which force companies to file premature updates rather than fix incidents. Converging around **a 72-hour substantive deadline and harmonising the trigger point, ensuring the clock starts ticking only when an incident is confirmed,** would improve both compliance and security; and
- **Simplify the CRA now**, by aligning application dates with the availability and citation of harmonised standards, allowing transitional self-assessment where appropriate, limiting reporting to the declared support period and excluding inherently low-risk products.

The Commission has started the simplification agenda; now the co-legislators must finish it. Deferring substantive corrections to future fitness checks risks losing the momentum that European industry urgently needs. The opportunity for real simplification exists, and must be seized, now.

[4] Directive 2002/58/EC, as modified by Directive 2009/136/EC.

[5] Directive (EU) 2022/2555, Regulation (EU) 2024/2847, Regulation (EU) 2022/2554, Directive (EU) 2022/2557, Regulation (EU) 910/2014 as amended by Regulation (EU) 2024/1183, and Regulation (EU) 2024/1689, respectively.

Table of contents

Rebalancing the Data Act

Europe's data legislation has grown into an intricate framework. The Commission's proposal to consolidate the Open Data Directive, the Data Governance Act and the Free Flow of Non-personal Data Regulation into the Data Act is a step towards greater coherence.[6] The merger aligns open-data and protected-data regimes under one structure, and gives administrations a more straightforward path for handling requests. The omnibus also strengthens the business-to-government (B2G) area by replacing the vague 'exceptional need' approach with a narrower 'public emergency' threshold, providing a clearer legal safeguard against routine or disproportionate demands.

For businesses, however, the effect is modest. The obligations that determine how firms can generate value from data, protect commercially sensitive information or develop and differentiate digital products are left untouched. These unresolved elements continue to have far greater implications for companies' bottom lines than the administrative clarifications offered in the omnibus.

The real test lies not in codification but in whether the rules enable companies to share and use data in ways that strengthen Europe's competitiveness. Two structural issues are particularly important.

A voluntary-by-default Data Act

As co-legislators amend the omnibus proposal, they must correct the structural flaw at the heart of the Data Act: mandatory, horizontal data-sharing obligations that do not reflect how European industries create value.

Many European manufacturers are still building viable data-driven service models. These depend on investment in digital capabilities, predictable commercial relationships and the ability to protect the value of the data services they develop. In sectors such as healthcare equipment, energy technologies, industrial machinery and advanced manufacturing, data is intrinsic to product design, maintenance cycles, safety assurance and aftermarket innovation. These data-enabled services are precisely where European companies can strengthen their competitive position globally, especially in the AI race. Forcing premature access and intervention into these business models, irrespective of commercial conditions or sectoral needs, undermines the very industries Europe needs to compete.

In sectors where data sharing has begun to scale, companies rely on negotiated contracts and established commercial relationships. Data exchange grows where there are a clear mutual benefit, technical feasibility and trust amongst participants rather than legal compulsion.[7]

For this reason, the co-legislators should **reverse the mandatory logic of the existing Data Act and replace it with a voluntary approach**. The most effective way to achieve this is through codes of conduct developed by industry. These codes can define the scope of access, protect sensitive information, set

[6] Directive (EU) 2019/1024, Regulation (EU) 2022/868 and Regulation (EU) 2018/1807, respectively.

[7] Examples include emerging sectoral data spaces where manufacturers, suppliers and service providers exchange operational and supply-chain data under negotiated agreements and shared governance models. Initiatives such as Catena-X in automotive, Manufacturing-X in industrial production, the recently launched Data4NuclearX project supporting safe and efficient nuclear-sector data exchange, and the Decade-X ecosystem for cross-domain energy, climate and industrial data all demonstrate voluntary, contract-based data sharing.

interoperability expectations and allocate responsibilities across the value chain. This model is already emerging organically, and the law should support, rather than constrain, these industrial initiatives.

The omnibus should therefore be amended to **give the Commission the power to recognise such sectoral codes**, allowing companies to opt in to a stable, trusted governance model where data access genuinely supports innovation and safety. This approach would enable data sharing where it delivers real value whilst avoiding the harmful consequences of compulsory openness in sectors that rely on long-term digital investment and protection of industrial know-how.

Full exclusion for software and platform services

When it comes to cloud portability, the omnibus proposes a narrow exemption for SaaS and PaaS contracts concluded before September 2025. This treats the issue as if the core difficulty were just the inconvenience of renegotiating past contracts. The real challenge is that imposing infrastructure-style portability obligations on software-based services fundamentally threatens the viability of these business models. These services represent a sizeable European part of the cloud market, whose competitive strength lies not in hyperscale infrastructure but in specialised SaaS and PaaS solutions.

For European SaaS and PaaS providers, the proposed portability framework touches the core of their business model. These services are highly specialised, require high customisation and complex configuration, and are tightly embedded in the architectural infrastructure and operational processes of sectors such as industrial manufacturing, healthcare technology, mobility, energy systems, and financial and professional services. Forcing portability in this context undermines differentiation and weakens incentives to invest in domain-specific innovation.

The proposed exemption for legacy contracts draws an arbitrary temporal line and does not address this structural incompatibility.[8] The only coherent solution is for the co-legislators to amend the omnibus so that **software- and platform-based services are fully excluded from the portability regime, with Chapter VI applying solely to infrastructure services** where switching is technically meaningful and commercially feasible. This would maintain the objective of promoting mobility in the cloud market without undermining the sectors where Europe has its strongest competitive advantage.

[8] The temporal design of proposed Art. 31(1a) compounds these problems. Under the current Data Act, companies have already been obliged to comply with the portability rules since 12 September 2025 – more than two months before the omnibus was put forward. The omnibus then proposes to exempt customised contracts concluded before that date, whilst leaving all contracts concluded afterwards – including those signed in the recent past – within scope. This means firms that acted responsibly to prepare for compliance may find that their renegotiated contracts were unnecessary, yet they must continue renegotiating others until the omnibus is agreed, if it is agreed at all. Because its adoption may take many months or even years, companies face prolonged uncertainty about which contracts will ultimately fall under the exemption, and which will not.

The exemption for SMEs and small mid-caps (proposed Art. 31(1b)) mirrors the temporal design for customised contracts: it applies only to agreements concluded before 12 September 2025. Contracts concluded after that date remain fully subject to the portability rules, even for smaller providers. This fragments the market without resolving the underlying issue. Providers must still redesign services for portability going forward, whilst attempting to navigate a retroactive exemption that may be adopted months or years after the cut-off date.

More fixes and provisions to delete

Trade secret safeguards

The omnibus leaves untouched the Data Act's core problem on trade secrets: the safeguards remain framed as exceptional defences that companies may invoke only in narrowly defined circumstances and only after satisfying an excessive procedural burden.

In substance, Arts 4(8) and 5(11) are left intact. The only change is an explicit reference to third-country risks that was already implicit in the original text.[9] The burden would still entirely lie on the data holder, including to assess trade secret protections in different jurisdictions. The provision remains framed as an exceptional defence requiring companies to demonstrate that 'serious economic damage' is 'highly likely,' and to notify authorities whenever they refuse access.

Trade secrets lose their value through exposure, not after a quantifiable loss occurs. Any disclosure to a party – whether inside or outside the EU – may compromise sensitive information irreversibly. Yet the Data Act continues to limit refusal grounds to exceptional, arguably predominantly third-country scenarios, leaving companies unable to rely on the safeguard in the settings where risks most commonly arise. This discourages firms from invoking legitimate defences and exposes them to avoidable commercial, cybersecurity and competitive risks.

The co-legislators should amend the omnibus so that **trade secrets and cybersecurity risks are treated as fully recognised grounds for refusing access without mandatory notification**. Where users believe a refusal is unjustified and would cause them disproportionate harm, they should be able to contest it before independent dispute-settlement bodies or, ultimately, before the courts. This would preserve normal business discretion whilst ensuring that oversight is applied to genuine disputes rather than to every instance in which a company chooses to protect the confidentiality of its assets.

Placement on the market

The omnibus does not address the Data Act's definition of 'placing on the market,' which presently might capture legacy product types that were designed and certified years ago but continue to be placed on the market over long delivery cycles. The Commission has already acknowledged this problem in the AI omnibus by clarifying, albeit only in a recital, that **products of the same type and model benefit from a grace period if at least one individual unit was lawfully placed on the market before the application deadline**.[10] A similar provision is needed under the Data Act, set out in a substantive provision.

Early termination

The omnibus would remove important flexibility that cloud infrastructure providers legitimately rely on. Today, Art. 29(4) Data Act allows all cloud providers to include early-termination penalties, so long as these

[9] The Commission's explanatory memorandum describes the omnibus amendment as a 'new rule' allowing data holders to refuse disclosure where there is a high risk of unlawful use or disclosure to third-country entities or EU entities under their control. However, current Data Act Arts 4(8) and 5(11) already call out enforceability of protections in third countries as a factor that may substantiate a refusal, without limiting the assessment to such jurisdictional risks.

[10] Recital 21 COM(2025) 836 final.

are disclosed upfront and are proportionate. However, proposed Art. 31(1b) could be read as instead prohibiting infrastructure services from doing so, whilst allowing software and platform services to continue.

Infrastructure contracts involve multi-year commitments to hardware capacity, energy supply, data-centre space and network resilience. Early-termination clauses are the mechanism that enables providers to offer customers lower prices for multi-year contracts. Without them, providers would have to price in the risk of sudden customer exit, making long-term offers more expensive or unavailable altogether. Restricting early-termination provisions for infrastructure services therefore harms both providers and customers, and creates an incoherent situation in which the only part of the cloud stack where switching obligations make sense is also the only one forbidden from using the contractual tools needed to support long-term investment. **Proposed Art. 31(1b) should therefore be deleted**.

Data transfers

As we have long demonstrated, Art. 32 Data Act duplicates the GDPR's transfer rules. Whilst the Data Act rules are framed as addressing non-personal data, they are in fact a response to scenarios that almost invariably involve personal data, and are therefore governed by the GDPR.[11]

The omnibus amends Art. 32 only to consolidate the categories of entities covered, reflecting the merger of several instruments into the Data Act.[12] The co-legislators should instead **delete Art. 32 in full** to avoid overlapping regimes.

Public-sector data fees

The omnibus introduces a new provision allowing public bodies to impose differentiated conditions for accessing open data, including higher fees, to 'very large enterprises,' to recover of the full cost of producing data and a return on investment.[13] This measure risks disadvantaging European industrial firms that depend on public-sector data for innovation and compliance, and will result in introducing 27 divergent pricing regimes and undermining Europe's objective of making public data widely reusable. Additionally, the proposal for public sector bodies to introduce different licence conditions for data reuse instead of using standard open licences would lead to incompatibilities and limit data reuse. The co-legislators should **delete this provision**.

Delay for product design requirements

Given the need to correct the Data Act's structural flaws, as well as delays in the publication of model contractual terms and in standardisation work, **the September 2026 deadline for designing products should be postponed by at least one year**.[14]

[11] See DIGITALEUROPE, *Data transfers in the Data Strategy: Understanding myth and reality*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2022/06/DIGITALEUROPE_Data-transfers-in-the-data-strategy_Understanding-myth-and-reality.pdf.

[12] Art. 1(16) of the proposal.

[13] Art. 32y in Art. 1(18), ibid.

[14] Art. 3(1) Data Act.

For safety-critical, security-sensitive and highly regulated products across sectors such as industrial machinery, automotive, medical devices or energy, some of which have hardware cycles of 3-4 years, design obligations without harmonised standards would fragment architectures, increase cybersecurity and privacy risks, undermine certifications and impose disproportionate costs, particularly on complex supply chains and SMEs.

GDPR: clarifying, not rewriting, a fit-for-purpose framework

DIGITALEUROPE's recommendations on the GDPR ahead of the digital omnibus were deliberately narrow. They focused on two points only:

- Clarifying the role of legitimate interest for innovation and security; and
- Clarifying that pseudonymised data may be considered non-personal for entities who have no access to, or legal means of obtaining, the re-identifying information.

The omnibus broadly takes up these recommendations and codifies existing guidance and case law. The revised definition of personal data in Art. 4(1) makes explicit that identifiability must be assessed in light of the means and legal powers available to each controller. This could be further accompanied by a clarification of whether data processing agreements would be necessary. In parallel, the new provisions on special categories and scientific research confirm that innovation uses can rely on the standard GDPR legal bases, including legitimate interest, rather than being treated as exceptional or suspect.

That our recommendations were so narrow is telling. For industry, the GDPR remains a fit-for-purpose horizontal framework that can evolve with technology. These are not attempts to reopen the GDPR, but to stabilise interpretations that industry has long advocated, yet have faced divergent enforcement practices and a reluctance amongst data protection authorities to recognise more progressive interpretations of the legal text. Recent case law and guidance confirm this direction of travel: identifiability must be assessed relative to the controller's means, and legitimate interest can support responsible data processing for innovation.[15]

Contrary to some of the more dramatic commentary, these changes do not alter the GDPR's guarantees, but make its interpretation more predictable at a time when European industry needs all the legal certainty it can get to invest in data-driven products and AI.

Where the omnibus goes in the right direction

Beyond our original asks, the omnibus introduces several clarifications we largely support.

First, the **amendments to Art. 9 on special categories of personal data** bring more context to how sensitive attributes can be processed in the development, testing and operation of AI systems. Proposed new Art. 9(2)(k) is intended to clarify that the processing of special categories of personal data may be lawful where necessary in an AI context, subject to appropriate safeguards. However, proposed Art. 9(5) risks significantly undermining this clarification. By requiring controllers to implement measures to avoid the collection and processing of special categories of personal data and, where such data are nonetheless identified, to remove them by default, Art. 9(5) treats the presence of special categories as a failure rather

[15] In particular, see the Court of Justice's judgment in Case C-413/23 P and the EDPB's Opinion 28/2024.

than as a legitimate and necessary condition. Art. 9(5) should be recast as a safeguards provision, allowing controllers to retain and protect special categories where necessary through proportionate technical and organisational measures.

In the same vein, the introduction of a **new Art. 88c usefully clarifies that the development and operation of AI systems and models may rely on legitimate interest**. Refinements to this provision, however, are needed. First, the reference to an 'unconditional' right to object should be removed in light of Art. 21(1) GDPR, which allows controllers to demonstrate compelling legitimate grounds that override the data subject's objection. Second, the provision allows other Union or Member State laws to displace Art. 88c by mandating consent. Third, clarification would be helpful to ensure that data minimisation during the 'selection of sources' does not unduly restrict the use of diverse datasets necessary for effective bias detection and mitigation.[16]

Similarly, we support the proposal to clarify the **conditions for processing biometric data** under Art. 9(2)(l), which usefully recognises privacy-preserving authentication models where biometric data remain under the data subject's control. The notion of 'sole control,' however, should be replaced with 'effective control' to avoid excluding privacy-preserving architectures such as hardware-secured, on-device biometric matching, where device manufacturers retain control over firmware or security updates. What matters is that only the data subject can authorise use of their biometric data and that no third party can access or repurpose biometric templates.

The introduction of a **clear, operative definition of 'scientific research'** finally gives legal weight to what Recital 159 states: that scientific research covers both public and private research efforts. This matters particularly for health and industrial research, where some authorities have been reluctant to accept that the GDPR can support responsible data use beyond narrow public-sector or academic settings. Clarifying the scope of research in the articles, not just in a recital, will help remove unjustified barriers that have held back projects that are fully compatible with the GDPR.[17]

The amendment to the right of access under Art. 12(5) GDPR helpfully recognises that some requests can be **manifestly unfounded or excessive**, clarifying that this includes harassment, fishing expeditions and procedural abuse, notably in pre-litigation contexts.

Last, we also support the intention to **harmonise data protection impact assessments and data breach notification practices**. Divergent DPIA lists and differing expectations around breach reporting have created uncertainty for companies operating across several Member States. The omnibus proposes to achieve this through Commission implementing acts.[18] For DPIAs, it is more consistent with the GDPR's governance structure to entrust this work to the EDPB, which is already responsible for ensuring consistent application of the Regulation. For breach notifications, a Commission-defined template can work only if it

[16] These GDPR amendments are being proposed alongside parallel in the AI omnibus; our recommendations to ensure consistency and avoid overlapping regimes can be found in our AI omnibus position, available at [add link when published].

[17] See DIGITALEUROPE, *Making the most of the GDPR to advance health research*, available at https://cdn.digitaleurope.org/uploads/2021/06/Making-the-most-of-the-GDPR-to-advance-health-research_DIGITALEUROPE.pdf.

[18] New proposed Arts 33(6)–(7) and 35(4)–(6c).

becomes part of a single, cross-regime incident-reporting template aligned with the emerging single entry point.[19]

Changes of limited practical value

Other GDPR amendments in the omnibus are, at best, of marginal practical importance.

The proposed changes to the **Art. 13 information requirements** are unlikely to resolve the real difficulty faced by controllers, which lies in finding a proportionate way to communicate complex information to data subjects. As we have previously argued in the context of access rights, the challenge is not the existence of the obligation but the need to strike a workable balance in terms of volume, granularity and intelligibility of information.[20]

Similarly, the proposed **restructuring of Art. 22 on automated decision-making**, which has already attracted strong public reactions, does not alter the substance of the provision. Controllers can rely on solely automated decisions with legal or similarly significant effects only under the same three conditions as today, and data subjects can therefore challenge decisions where those conditions are not met. The mere removal of the word 'right' from the text does not change this.

We also see no added value in creating a **new Art. 41a empowering the Commission to adopt implementing acts on anonymisation**. The clarification introduced in the definition of personal data in Art. 4(1) is already a significant step forward to allow controllers and authorities to support the use of privacy enhancing technologies and to assess, case by case, whether data should be considered personal or anonymous. Whilst we support greater harmonisation, the GDPR's architecture means that this work should remain with the EDPB, which is tasked with ensuring consistent application and developing common guidance. Adding a parallel layer of Commission implementing acts would cut across that role and risk undermining the case-by-case approach that the new definition is meant to support.

Finally, the proposal to **extend the breach notification deadline from 72 to 96 hours** reflects a legitimate concern about the pressure that short reporting timelines place on organisations. However, in the current regulatory landscape it would not deliver meaningful relief. DIGITALEUROPE has been calling for alignment around the GDPR's 72-hour standard in an environment where other regimes have started to require much faster notifications followed by several updates.[21] Shifting the GDPR deadline to 96 hours does not address this wider fragmentation; instead, it risks undermining the only relatively stable point of reference in the system whilst leaving the underlying timeline problem across cyber legislation untouched.

The unresolved issue: ePrivacy and terminal equipment data

[19] See 'One harmonised template, not many' section below.

[20] See DIGITALEUROPE, *Balancing rights and obligations for an effective GDPR access right*, available at https://cdn.digitaleurope.org/uploads/2022/03/Balancing-rights-and-obligations-for-an-effective-GDPR-access-right.pdf.

[21] Both NIS2, CER and the CRA require an early warning within 24 hours of awareness, pushing companies to submit speculative or incomplete information. This is followed, for NIS2 and the CRA, by a more detailed report within 72 hours; a final report is required one month after notification under all three laws. DORA goes further by stipulating a four-hour deadline for financial entities' initial notifications, with a 72-hour update and a final report after one month.

By far the most problematic part of the omnibus lies not in the GDPR amendments themselves, but in the partial integration of ePrivacy rules.[22]

ePrivacy governs all processing of terminal equipment data – not just cookies and online advertising, but any reading from or writing to a device, and the collection of information from it. The political debate has often reduced this to banners and tracking, but the legal scope is much wider. For years, we have advocated subsuming processing of terminal equipment data under the GDPR, so that controllers can rely on the GDPR's risk-based framework and full range of legal bases. Crucially, this includes legitimate interest for uses such as security or product safety, service improvement and research. This is **essential not only for consumer services but also for industrial environments**, where ePrivacy currently applies to device and machine data that's critical to the competitiveness of Europe's industrial sectors.

The omnibus repeats the approach already tried in the failed ePrivacy Regulation.[23] It leaves the separate, consent-centred regime in place and seeks to solve the problem by expanding exceptions to consent – for transmission, basic service provision, certain security and measurement functions. This cannot accommodate the full spectrum of legitimate uses of device data that companies must pursue, including in industrial environments.

Worse, the omnibus creates a perverse asymmetry. Whilst it brings personal data from terminal equipment under the GDPR, it leaves anonymous terminal equipment data under the old ePrivacy rules. This means less intrusive processing – of data that does not identify individuals – is subject to more stringent requirements than the processing of personal data. This is illogical, and will incentivise controllers to keep data identifiable rather than anonymise it.

Proposed Art. 88b, which seeks to mandate machine-readable consent signals and technical measures at device or software level, also reprises another unresolved debate from the failed ePrivacy negotiations. There is no shared technical foundation for such a system, and no clear link to existing standards work. Moreover, this system would make consent the only *de facto* mechanism for processing terminal equipment data: the software layer becomes a gatekeeper that blocks any operation for which no signal has been given. This will prevent controllers from processing device data, even where allowed on another legal basis.

The only coherent solution is to **bring all processing of terminal equipment data fully under the GDPR's legal bases**, and to phase out the parallel ePrivacy regime for device access. Anything short of full incorporation will continue to disincentivise the responsible use of terminal equipment data.

Cyber: a single entry point without real simplification

On cyber, the omnibus focuses on *how* companies report incidents, not *what* or *when* they must report. It tasks ENISA with developing a single entry point through which notifications under the GDPR, NIS2, DORA,

[22] Proposed Art. 88a.

[23] See, in particular, pp. 2-3 of *DIGITALEUROPE's consolidated position on ePrivacy Regulation*, available at https://cdn.digitaleurope.org/uploads/2019/01/DIGITALEUROPE%E2%80%99s%20consolidated%20position%20on%20ePrivacy%20Regulation.pdf.

eIDAS and CER would be submitted. That is a useful step, but it is only a starting point. The omnibus falls short of the broader simplification package we proposed.[24]

A key problem is the architecture of timelines. Over the past years, the GDPR's 72-hour notification requirement has become the *de facto* reference point for incident reporting. NIS2, CER, the CRA and DORA have layered on top of this a cascade of early warnings within 24 hours – or even 4 hours in the case of DORA – followed by intermediate and final reports. The omnibus proposal solidifies this multi-step model, which is the real problem.

Whilst we appreciate the intention to support early cybersecurity reactions, the reality for companies is an avoidable layer of red tape: resources are diverted from investigating and containing incidents to producing multiple mandatory updates, and authorities are flooded with premature or incomplete reports they cannot meaningfully act on.

A more coherent approach would be to **converge around a flexible 72-hour deadline** as the common standard – allowing entities to report earlier where they can and where it adds value – so that companies and authorities can focus on remedying incidents rather than reporting them.[25] This approach will also improve administrative efficiency and increase the accuracy of reports.

Furthermore, the Commission's proposal amends Art. 23(12) NIS2 to exempt incidents reported under the CRA from additional NIS2 notification, where the reported information overlaps. This provision should be reciprocal, ensuring that incidents reported under NIS2 also do not require separate reporting under the CRA, and should be extended to overlapping reports under other legislation, where possible.

Art. 12 CRA states that high-risk AI systems complying with the CRA's essential requirements will be deemed compliant with Art. 15 AI Act, where in scope of both regulations. However, the AI Act's conformity assessment procedure still needs to be followed in such case. There should be a clear provision stating that compliance with either regulation – and its corresponding reporting obligations – should be sufficient.

Regarding DORA, financial entities already operate under a highly mature and intensive supervisory framework, where incident reporting is closely linked to real-time supervisory engagement and operational remediation. Allowing DORA notifications to be submitted via the single entry point will reduce duplication and support convergence across regimes, provided that existing sector-specific incident reporting rules are no longer maintained following the implementation of the single entry point. Financial entities remain concerned that financial authorities will continue to impose parallel or additional reporting obligations beyond those envisaged in the omnibus proposal, resulting in dual reporting and defeating the objectives of the omnibus.

Finally, we echo concerns expressed by some Member States on how ENISA will be able to ensure the security of all the information entities will be submitting through the single entry point, as this will lead to a 'honeypot' risk. Additional funding and resources for ENISA so that sensitive information is secure and not vulnerable to attacks is needed.

---

[24] See DIGITALEUROPE, *Digital simplification package: Our cyber recommendations*, available at https://cdn.digitaleurope.org/uploads/2025/10/071025-Digital-simplification-package-Cyber.pdf. In particular, pp. 2–6 set out our detailed recommendations on incident reporting and notification. For the purposes of this paper, we limit ourselves to summarising the main elements.

[25] Art. 73 AI Act establishes the deadlines for the reporting of serious incidents. These are not covered by our call to converge the reporting timelines around 72 hours as the common deadline.

A truly single entry point

The current list of regimes feeding into the single entry point is incomplete. It should also **include the AI Act**, as incidents involving AI systems will have a clear security or safety dimension. In parallel, ENISA is already mandated to develop the **CRA single reporting platform** for severe incidents and vulnerabilities: the omnibus must unequivocally **commit to using that platform** as the single entry point.

One harmonised template, not many

Recital 54 acknowledges the value of standardised templates developed under DORA and suggests they should be 'taken into account' when designing notifications for the single entry point under NIS2, CER and the GDPR. However, this remains a high-level instruction in a recital and will not prevent different templates emerging under each instrument; it does not even refer to the CRA, where the Commission is also empowered to define notification formats.

The omnibus should **mandate a single core incident-reporting template**, with limited sector-specific additions. This will avoid a proliferation of slightly different templates. The core template should be based on international standards and cover the format, incident description, impact, mitigation and follow-up measures, with optional fields for regime-specific requirements, so that a single report can satisfy all relevant frameworks. This includes harmonised templates issued under NIS2, where these currently differ per Member State.

Unified incident thresholds

Importantly, the compliance burden for organisations often relates to the incident reporting criteria, thresholds and data fields required across each reporting stage. Effective simplification hinges on streamlining and reviewing the complex reporting criteria.

The digital omnibus should **establish a harmonised threshold to determine when an incident is significant** enough to warrant reporting. This would ensure consistency whilst still allowing each regulation to apply the threshold within its specific context. The most appropriate baseline is the NIS2 notion of a 'significant incident,' defined by severe operational disruption or substantial damage.

Substantive simplification must not be deferred

The Commission has signalled that more ambitious changes may follow after the ongoing digital fitness check and in future omnibuses.[26] Whilst we welcome this acknowledgement, industry is already clear and specific about the adjustments needed, based on day-to-day experience of building and operating the products and services that these rules govern. Fragmenting simplification across several future packages is not a sustainable approach. As much cyber simplification as possible should be explored for inclusion in this omnibus by the co-legislators.

[26] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/15554-Digital-fitness-check-testing-the-cumulative-impact-of-the-EUs-digital-rules_en.

Cyber Resilience Act

Compliance with the CRA will be very challenging. Across the entire value chain, many actors are struggling to be fully prepared to comply within the required timeframe. Compliance will depend on extensive due diligence of third-party components, requiring unprecedented coordination amongst manufacturers. If any link in the chain is not ready in time, the result could be delays, disruptions or shortages of essential components.

The omnibus does not touch the CRA's complex obligations on scope, essential requirements, conformity assessment or interaction with sectoral legislation, such as DORA, despite the concrete adjustments we have suggested.[27] These include aligning application with the availability and citation of harmonised standards, supporting self-assessment for important products during the transition, limiting reporting to the declared support period, providing a transition for RED-compliant products,[28] tailoring requirements for industrial systems and excluding inherently low-risk products.

Nor does it move towards an EU-wide coordinated vulnerability disclosure policy that better links the CRA reporting platform with the European vulnerability database and removes the risky obligation to report unpatched vulnerabilities.[29]

This means that the parts of the cyber rulebook that are most impactful for business models and security operations are left intact, whilst legislative attention is spent on the portal through which companies must navigate them. The co-legislators should therefore use the legislative process to insert further measures that are necessary for genuine simplification.

As noted, the CRA necessitates the development of a substantial number of both vertical and horizontal standards. Progress in standardisation, which is particularly complex in the CRA's case, faces nearly impossible deadlines, making delays very likely. For this reason, the Commission should proactively provide for a **postponement of the CRA compliance deadline by at least one year**, extending it to December 2028.

NIS2 Directive

NIS2 transposition into national legislation remains highly fragmented, resulting in challenges for cross-border operators. Besides harmonised reporting templates, several issues require harmonisation.

As argued above, the NIS2 baseline of 'significant incident' provides the most appropriate baseline around which other incident definitions should converge. That does not mean its implementation has been effective so far. Some Member States do not adhere to the threshold set out by the NIS2 implementing act.[30] This

[27] The Commission's proposal focuses solely on the creation of a single entry point. As such, it addresses only one element of our June recommendations on cyber simplification. Those recommendations remain fully valid. In this paper, for reasons of brevity, we list only the main ones. A comprehensive presentation of DIGITALEUROPE's CRA recommendations can be found in *Digital simplification package: Our cyber recommendations*, pp. 7–10.

[28] Directive 2014/53/EU.

[29] See DIGITALEUROPE, *Digital simplification package: Our cyber recommendations*, pp. 6–7.

[30] Implementing Regulation (EU) 2024/2690.

requires reports for virtually any incidents to competent authorities. The omnibus should further enshrine thresholds for significant incidents.

The fundamental principle of main establishment must be consistently applied. In practice, interpretations vary between Member States, subjecting critical entities to multiple jurisdictions where the Directive did not intend so. Besides, the omnibus should clarify that the main establishment principle applies to operators providing ICT services and simultaneously falling in Annex II.

FOR MORE INFORMATION, PLEASE CONTACT:

Béatrice Ericson

Manager for Data Economy, Privacy & Public Administration

beatrice.ericson@digitaleurope.org / +32 490 44 35 66

Julien Chasserieau

Associate Director for AI & Data Policy

julien.chasserieau@digitaleurope.org / +32 492 27 13 32

Sid Hollman

Policy Manager for Cybersecurity, Digital Infrastructure & Mobility

sid.hollman@digitaleurope.org / +32 491 37 28 73

Alberto Di Felice

Policy and Legal Counsel

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory and investment environment that enables European businesses across multiple sectors, as well as citizens, to prosper through digital technologies. We wish Europe to grow, attract and sustain the world's best digital talent, investment and technology companies. Together with our members, we shape industry positions on all relevant policy matters, and contribute to their development and implementation. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes corporations and scaleups which are global leaders in their fields, as well as national trade associations from more than 30 European countries.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20