DIGITALEUROPE

THE EXECUTIVE BRIEF:

REMOVING REGULATORY BURDEN FOR A MORE COMPETITIVE AND RESILIENT EUROPE

Europe's tech future is a geopolitical imperative. Staying competitive in critical technologies like AI, quantum computing and advanced semiconductors is essential for our economic resilience, defence capability and global relevance. Whilst Europe holds strong supply chain positions in energy tech, advanced manufacturing, health biotech and space, it lags global competitors in 7 out of 8 strategic technology areas.[1]

The main barrier is not talent or market size. We have a vast market of 440 million consumers and 23 million companies,[2] account for 15 per cent of global GDP, file 17 per cent of the world's patent applications,[3] and are home to 18 per cent of top-tier AI talent.[4] The problem lies in our inability to scale and commercialise innovation. Fragmented markets, non-scalable national incentives and procurement schemes, and – above all – overly complex regulation are holding us back.[5]

This paper addresses the regulatory dimension. It offers practical proposals to reduce unnecessary burdens in AI, data and cybersecurity rules. There is broad consensus amongst CEOs that regulatory simplification would be the single most powerful lever to boost investment and innovation in Europe.

Acknowledging this, the Commission has committed to reducing reporting obligations by at least 25 per cent for large companies and at least 35 per cent for SMEs by the end of its mandate in 2029. DIGITALEUROPE calls for bolder cuts of 50 per cent for Europe's industry to stay competitive, in line with Draghi's recommendations.

The upcoming digital simplification package presents a timely opportunity to implement targeted reforms. By focusing on three critical areas – data, artificial intelligence and cybersecurity – we can enact low-hanging, high-impact changes that will:

- **Simplify complex and overlapping regulations to reduce administrative burdens;**
- **Enhance legal clarity and coherence across Member States; and**
- **Strengthen Europe's capacity to scale and compete globally.**

This comprehensive proposal outlines our key recommendations in each of these areas, aiming to build a more agile, competitive and technologically sovereign Europe.

Cecilia Bonefeld-Dahl
Director General
DIGITALEUROPE

Peter Weckesser
President
DIGITALEUROPE
Chief Digital Officer, Schneider Electric

Doris Pold
Vice-President
DIGITALEUROPE
CEO, ITL

---

[1] See DIGITALEUROPE, *The EU's critical tech gap: Rethinking economic security to put Europe back on the map*, available at https://cdn.digitaleurope.org/uploads/2024/07/DIGITALEUROPE-CRITICAL-TECHNOLOGIES-REPORT-FINAL_JULY_WEB.pdf.

[2] Mario Draghi, *The future of European competitiveness – Part A: A competitive strategy for Europe.*

[3] Eurostat, *Key figures on The EU in the world*, 2025 edition.

[4] European Economic and Social Committee, 'Artificial intelligence: 18% of the world's top-tier researchers are European, but only 10% work in Europe,' available at https://www.eesc.europa.eu/en/news-media/press-releases/artificial-intelligence-18-worlds-top-tier-researchers-are-european-only-10-work-europe.

[5] ERT, *The Conference Board Measure of CEO Confidence™ for Europe*, November 2024.

Over the past five years, Europe's digital landscape has been shaped by nearly 40 new regulations, often overlapping and inconsistent, which have raised compliance costs and hampered innovation.

Some figures illustrating the burden:

€60.2 billion

a year in compliance costs for CRA and NIS2 alone[6]

€3.3 billion

annual cost to comply with the AI Act, assuming 10% of AI products are subject to it[7]

15%

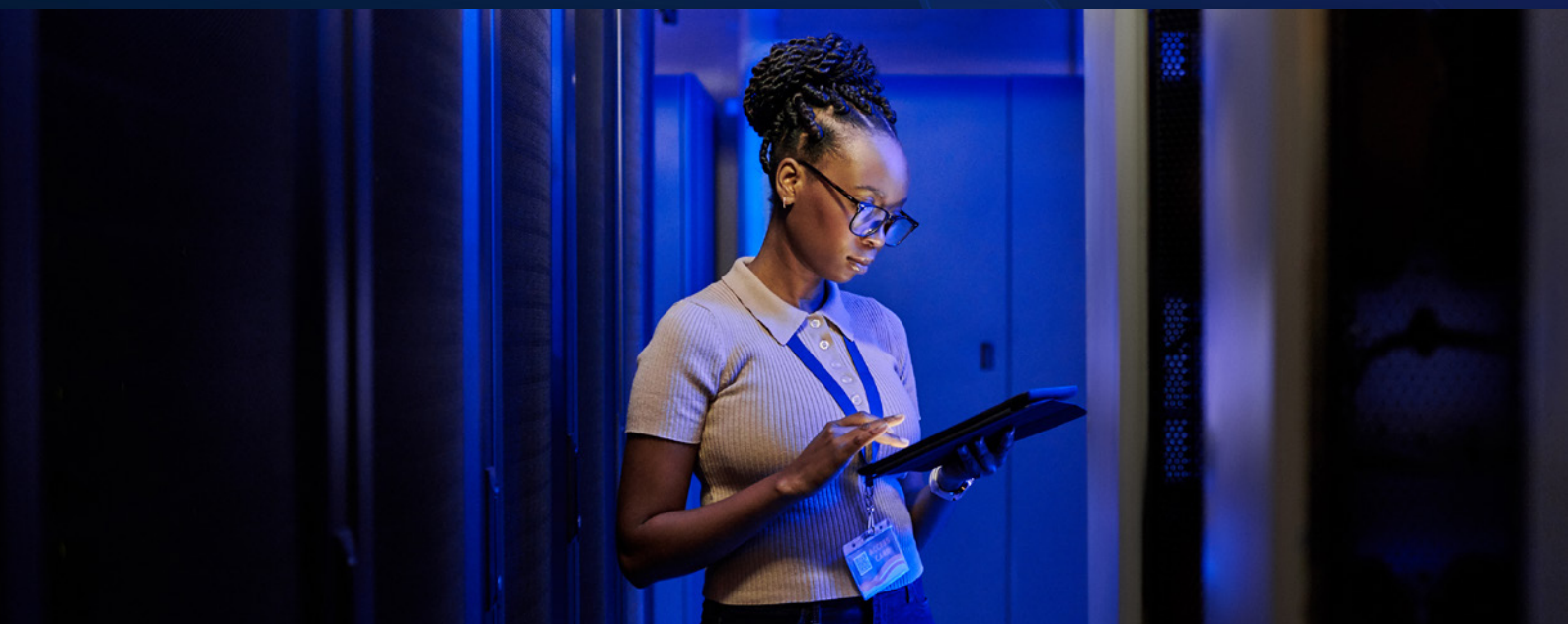
profit loss for small tech firms due to GDPR fragmentation[8]

€235 million

recurring annual costs to comply with Data Act data sharing obligations[9]

13%

increase in overall compliance costs over past 5 years according to DIGITALEUROPE's members[10]



[6] Frontier Economics, *Assessing the economic impact of EU initiatives on cybersecurity and SWD*(2022) 282 final.

[7] ICF, CEPS and Wavestone (2021), *Study supporting the impact assessment of the AI regulation.*

[8] Mario Draghi, *The future of European competitiveness.*

[9] SWD(2022) 34 final.

[10] DIGITALEUROPE surveyed its members in October 2024 on the evolution of legal and compliance costs impacting their operations in Europe. 109 members participated in this survey.

RECOMMENDATIONS BY AREA

Data

Europe's data framework has grown increasingly complex, going beyond the well-established General Data Protection Regulation (GDPR) with overlapping rules like the Data Act and Data Governance Act (DGA) that impose significant burdens on businesses. These regulations often criminalise data markets before they fully develop, creating a burdensome environment around data sharing and governance. To avoid compounding these challenges, the application of the Data Act should be postponed to allow time for simplification under the upcoming digital package.

BUSINESS CASE: REGULATORY BARRIERS TO AI INNOVATION IN EUROPEAN HEALTHCARE

An innovative healthcare company from DIGITALEUROPE's membership has created an AI tool that records and transcribes doctor-patient consultations live, so doctors can focus on the conversation instead of note-taking. To keep raising the tool's accuracy, the company must train its AI model on real transcripts that have been pseudonymised or anonymised.

The GDPR makes that difficult. Health data falls under Art. 9 special category rules, and the only clear legal basis to anonymise or pseudonymise it is the patient's explicit consent. Securing consent for every transcript is unrealistic: many patients are reluctant to share their health data to train an AI model they do not fully understand. As a result, the company cannot feed enough examples into its model, slowing improvements that would benefit doctors and patients alike.

The AI Act does not consider support tools like this as 'high-risk,' but these beneficial use case are anyway curtailed by the GDPR. Unless a risk-based alternative to consent is provided to process health data, European health innovators will trail competitors in less restrictive markets and patients will miss vital benefits of AI-enabled care.

Main recommandations

- **Adopt a voluntary approach to data sharing:**
  - Make data sharing under the Data Act voluntary by default, supporting Europe's industrial innovation.
  - Empower the Commission to recognise industry-developed codes of conduct, allowing tailored data-sharing frameworks for different types of connected devices.
- **Strengthen trade secrets and cybersecurity protections:**
  - Recognise trade secrets and cybersecurity as fully legitimate grounds to withhold data under the Data Act, without triggering mandatory notifications.
  - Shift the burden of contesting refusals to the requester, rather than the data holder.
- **Clarify temporal scope:**
  - Amend the Data Act's definition of 'placing on the market' to exclude legacy products, developed years ago but placed on the market over long delivery timelines (e.g. vehicles, aircraft).
  - Apply data sharing obligations only to future contracts, preventing disproportionate retroactive effects.
- **Radically simplify governance:**
  - Designate a single competent authority per Member State. This authority should handle all administrative functions under the Data Governance Act (DGA), including support to public sector bodies, notifications from intermediation services and registration of data altruism organisations.
  - Task this same authority with authorising the independent dispute resolution bodies, which should become the sole venue for resolving all disputes under the Data Act.
- **Delete overlapping data transfer rules:**
  - Delete redundant international data transfer provisions in the Data Act, the DGA and the European Health Data Space (EHDS), which duplicate GDPR protections.
- **Ensure practical cloud rules:**
  - Restrict portability requirements to infrastructure services to support Europe's development of industrial solutions across sectors such as healthcare, energy, manufacturing, finance and retail.
  - Allow more flexible transition periods for switching, recognising that migrations are often complex and iterative.
- **Clarify the GDPR without reopening it:**
  - Reinforce the use of 'legitimate interest' as a ground to process personal data for key use cases such as product development – including of AI models – and security.
  - Clarify that pseudonymised data is not personal data when recipients cannot reasonably re-identify individuals.

Artificial intelligence

The AI Act represents the most comprehensive AI regulatory effort globally, ensuring that AI systems deployed in Europe are safe, transparent and aligned with fundamental rights. However, its extensive scope and complexity pose significant challenges for industry compliance, particularly when it comes to harmonised standards, conformity assessments and the interaction with sector-specific legislation.

BUSINESS CASE 1: AI ACT & GDPR COMPLIANCE CATCH-22 PUTS PROJECT ON HOLD

A European IT consultancy has developed an AI tool to help a government agency screen job applicants more fairly. Under the AI Act, AI-enabled recruitment tools are deemed high-risk and must undergo rigorous bias testing. In practice that means feeding the model sensitive attributes such as ethnicity. Yet, the GDPR classifies ethnicity as a special category of personal data that requires each candidate's explicit consent – an impractical ask. This regulatory contradiction forces the company to abandon the project as satisfying the AI Act's bias mitigation requirements would breach the GDPR, exposing the company and its client to potentially very high fines.

BUSINESS CASE 2: UNCERTAINTY OVER GPAI PAPERWORK THREATENS AI PLATFORM

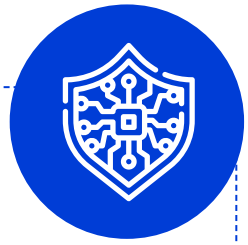
One of Europe's largest automotive companies has built a self-service generative AI platform that enables employees to automate specialised tasks, from process analysis and optimisation to document interaction. The tool has seen a strong uptake, generating more than 300 app instances every week. However, under the AI Act, any app that incorporates company data or tweaks prompts risks being classified as a new generative AI model, triggering burdensome documentation requirements that outweigh the platform's productivity gains. Excluding downstream modifications and fine-tuning from provider and deployer obligations is critical to supporting AI adoption.

Main recommandations

- **Integrate AI requirements into sectoral laws:**
  - Instead of applying the AI Act directly to products like machinery, medical devices or radio equipment, which are already covered by comprehensive sectoral rules, allow the Commission to introduce AI requirements through these existing frameworks when necessary. This would align all Annex I products with the more flexible approach already used for some of them (Section B).
- **Apply only when harmonised standards are available:**
  - Delay the application of high-risk AI requirements until at least 12 months after relevant harmonised standards are published, allowing sufficient time for adaptation.
  - Eliminate the adoption of common specifications, which would undermine the successful development of harmonised standards.
- **Expand the legacy clause:**
  - Exempt AI systems already on the market (including GPAI models) from new compliance obligations unless there are significant changes to their design.
- **Remove unnecessary registrations, assessments and oversight:**
  - Abolish the mandatory registration of AI systems, along with the related EU and Member State databases.
  - Replace fundamental rights impact assessments (FRIAs) with data protection impact assessments (DPIAs), which are already mandated by the GDPR.
  - Delete uniform Commission-issued template for post-market monitoring plans, allowing providers to design plans adapted to their AI systems and risk contexts.
  - Protect intellectual property and cybersecurity by ensuring that authorities are not granted access to source code.
  - Remove Member States' power to impose unilateral additional obligations, which undermines legal certainty and the single market.
- **Clarify how GPAI rules apply to deployers:**
  - Clarify that deployers are only considered GPAI model providers when substantial modifications result in a new general-purpose model.
- **Strengthen AI governance:**
  - Transform the AI Office into an independent body with EU-wide supervisory powers to avoid political influence and ensure consistent implementation.
  - Establish an Industry Advisory Council to provide practical business insights.

- **Empower sandboxes to grant presumption of conformity:**
  - Grant presumption of conformity for AI systems successfully tested in sandboxes, incentivising proactive participation by companies.
- **Protect innovation-friendly practices in AI development:**
  - Ensure the research exemption applies to all R&D phases, including commercial research, as long as the AI system is not yet placed on the market.
  - Align rules on using sensitive personal data to fix bias in AI systems with the GDPR's more flexible interpretation; allow retention of personal data for ongoing bias monitoring; and permit data re-use in sandboxes even outside of narrow public interest cases.
  - Confirm that open-source licences with responsible use clauses qualify for the open-source exemption, and that open-source components retain their exemption when integrated into proprietary AI systems.

Cybersecurity



Europe's cybersecurity framework has become highly fragmented, with overlapping reporting requirements from multiple regulations such as NIS2 and the Cyber Resilience Act (CRA), as well as sectoral frameworks like DORA for finance. This fragmentation imposes significant compliance burdens on businesses. To strengthen Europe's cyber resilience, the digital simplification package should streamline reporting processes, harmonise compliance frameworks and support a more coordinated approach to cybersecurity governance.

BUSINESS CASE 1: COMPLIANCE BURDEN SIPHONS SECURITY RESOURCES

A European health technology firm with a global footprint dedicates ten full-time employees exclusively to meeting NIS2 obligations – about 5 per cent of its global cybersecurity budget, counting both personnel and direct spend. To navigate the maze of overlapping reporting requirements, the company had to hire external specialists for an in-depth gap analysis. Similarly, a European IT-consultancy with roughly 2 300 employees maintains a seven-person team and pays an extra €100 000 each year for external audits just to ensure compliance with NIS2.

BUSINESS CASE 2: FRAGMENTED EU CYBER RULES DRIVE COSTLY REPORTING OVERLOAD

A Dutch bank must comply with five partially overlapping cybersecurity frameworks: DORA, NIS2, the Cyber Resilience Act (CRA), the Cybersecurity Act (CSA) and the EBA ICT Guidelines – each with different reporting fields, severity thresholds and deadlines.

Under DORA alone, a single major incident can trigger up to 16 separate notifications, each demanding as many as 105 distinct data points. Lacking standardised APIs, every report is compiled and uploaded manually to national portals, turning compliance into an expensive and error-prone paperwork exercise.

Main recommendations

▶ Establish a unified reporting framework:

- Introduce a harmonised threshold for reporting of significant incidents, based on NIS2.
- Align incident reporting timelines with the 72-hour GDPR model to allow a thorough initial assessment before notification, removing premature early warnings.
- Create a single, harmonised reporting template applicable under NIS2, the CRA, the GDPR and other laws.

▶ Create a reporting one-stop shop:

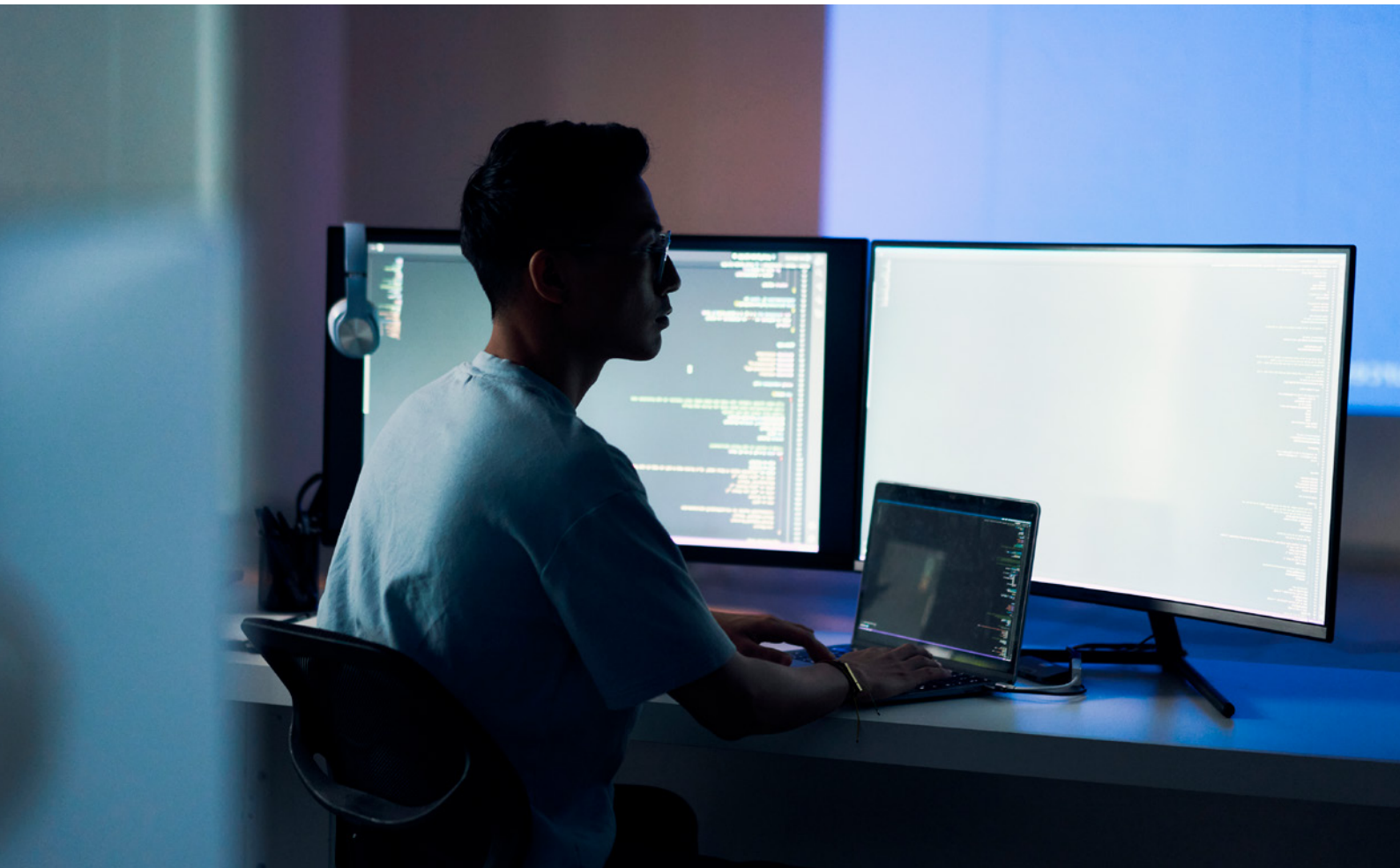
- Strengthen the new single reporting platform managed by ENISA to cover all relevant regulations, with automatic routing to national authorities.
- Mandate that Member States designate the same entity (preferably the national CSIRT) as both the CRA electronic notification endpoint and the NIS2 single point of contact.
- Set a mutual recognition policy requiring Member States to accept NIS2 compliance audits carried out under another country's national framework.

▶ Establish an EU-wide coordinated vulnerability policy:

- Establish a unified coordinated vulnerability disclosure process that integrates the single reporting platform and the European vulnerability database managed by ENISA.
- Remove the obligation to report actively exploited, unpatched vulnerabilities, which could expose attack vectors and pose significant security risks.

▶ Make CRA obligations more manageable:

- Delay the application of CRA essential requirements until 12 months after relevant harmonised standards for Annex I are published.
- Allow companies to self-assess important products until harmonised standards for these products are available and notified bodies in place.
- Limit reporting obligations to products' declared support period, avoiding burdens linked to obsolete or unsupported systems.
- Introduce a three-year transition period under which products already compliant with Radio Equipment Directive (RED) cybersecurity rules are automatically considered compliant with the CRA.
- Adapt CRA rules for industrial systems by clarifying that the spare parts exemption covers full product replacements and software tools, and by allowing alternative security solutions where full compliance is not technically feasible.
- Exclude simple, low-risk products – like toothbrushes and basic sensors – that do not pose real cybersecurity threats.



DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies.

We wish Europe to grow, attract and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies.

Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 108 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.


@DIGITALEUROPE


@digitaleurope_org


DIGITALEUROPE


@DIGITALEUROPEvideo

www.digitaleurope.org