Charter of Trust

Digital Package – Digital Omnibus
Public consultation

Publication date:14 October 2025

Executive Summary

This position paper from the Charter of Trust responds to the European Commission's public consultation on the Digital Omnibus Package. The rapid expansion of EU digital regulation has strengthened security, privacy, and trust, but it has also created overlapping obligations, inconsistent timelines, and administrative complexity. The Digital Omnibus Package provides a timely opportunity to streamline these rules, ensure greater coherence, and enable businesses to focus resources on resilience and innovation rather than redundant compliance tasks.

The Charter of Trust welcomes the Commission's initiative to harmonize digital regulations across the EU, aiming to reduce administrative burdens while maintaining high standards of security and privacy. Representing the unified views of its Partners, this paper addresses all key legislation within the scope of the Digital Omnibus and offers comprehensive recommendations. It emphasizes the need for a unified incident reporting system, risk-based notification requirements, and fair compliance processes to minimize regulatory overlap. The Charter calls for clearer liability clauses, global recognition of certifications, and stronger supply chain security.

In data regulation, the Charter advocates ensuring alignment between the rules on data intermediation services under the DGA and B2B data sharing under the Data Act and extending exemptions to mid-cap companies, all while safeguarding trade secrets. For artificial intelligence, the paper recommends a phased approach to new requirements, integrated conformity assessments, harmonized compliance templates, and clear definitions, supported by sector-specific guidance and transparent AI categorization. The Charter also encourages the European Commission to ensure that ePrivacy reform is future-proof, fosters innovation, and reflects the needs of both businesses and consumers. Finally, it recommends robust security standards and cross-border recognition for the EU Business Wallet, with industry involvement in technical standards and integration with data access systems.

Collectively, these measures are designed to foster innovation, resilience, and trust in the EU's digital landscape, allowing businesses to thrive in a coherent and future-ready regulatory environment.

Cybersecurity simplification agenda

We welcome the objective of the European Commission to streamline reporting obligations to reduce overlaps and administrative burdens on businesses through the proposal of the Digital Omnibus Package. Clear and concise reporting requirements will facilitate compliance and improve overall cybersecurity resilience.

The European Union has introduced a suite of cybersecurity legislative acts designed to enhance digital resilience across sectors. These include the NIS2 Directive, the Cyber Resilience Act (CRA), the Cybersecurity Act and the Digital Operational Resilience Act (DORA). While each instrument targets specific aspects of cybersecurity, their combined implementation has revealed significant challenges, particularly around incident reporting, regulatory overlap and supply chain security.

The European Commission's objective to harmonise cybersecurity incident reporting through the Digital Simplification Package is essential to addressing the current complexity. Businesses are currently subject to multiple reporting regimes under the GDPR, NIS2, the NIS2 Implementing Regulation, the Cyber Resilience Act (CRA), and the Digital Operational Resilience Act (DORA), each with different thresholds, timelines, and content requirements. This fragmentation leads to inconsistent and supplicative reporting, placing unnecessary burdens on companies and diverting essential cybersecurity resources away from mitigation, response and recovery efforts – ultimately weakening the EU's overall cyber resilience.

Key recommendations:

- **Single, harmonized reporting regime:** To address this complexity, we propose a single, harmonised reporting regime based on a one-stop-shop principles, allowing businesses to report incidents through a single point of entry, ideally in the country of main establishment. This approach should apply to all entities that are in scope of several legal acts (e.g. NIS2 and CRA). For example, incidents under CRA, NIS2 and sector specific legislation should be reported to ENISA which shall inform sectoral regulators where appropriate.

- **Risk based and proportionate notification requirements**: In addition, incident notification requirements should be risk-based and proportionate, with clearer definitions of incident severity thresholds, which are based on impact on confidentiality, integrity or service availability. This would allow businesses to fulfil their regulatory obligations primarily through one national authority in the EU, which will pass on the required information to ENISA and other responsible EU-level authorities, thereby streamlining reporting and enforcement.

- **Fair compliance process**: Before any enforcement action is taken for non-compliance or failure to report an incident, businesses should be given a reasonable opportunity – following regulator notification – to meet their legal obligations by submitting a compliant incident report. This approach would support a fair and constructive compliance process, especially as companies adapt to evolving regulatory requirements.

- **Clarification of liability clauses**: Both NIS2 and CRA are missing liability clauses which are necessary for allowing the information to be shared in a more controlled manner. While Art 23(1) of NIS2 points that notification shall not subject the notifying entity to increased liability, the law should also clarify that they should not be liable for potential spill-over effects caused by the act of notification.

- **Global interoperability and Mutual Recognition Agreements (MRA):** Europe's regulatory leadership in digital policy must be matched with global interoperability. The Commission should actively pursue Mutual Recognition Agreements with key international partners, ensuring that certification results conducted under recognized international accreditation systems (ILAC/IAF) are accepted across jurisdictions. This would reduce duplication for global manufacturers and reinforce the EU's competitiveness in digital markets.

Data acquis

The EU has developed an ambitious suite of data laws - including the Data Governance Act (DGA), the Data Act, the Free Flow of Non-Personal Data Regulation, and the Open Data Directive - with the shared aim of fostering data-driven innovation. However, the resulting acquis has become fragmented and difficult to navigate, creating compliance complexity for businesses while falling short of its potential to unlock trusted data sharing.

As Charter of Trust partners, we support the Commission's objective to consolidate and simplify these frameworks. Streamlining rules will strengthen legal certainty, enable data-driven innovation, and support Europe's competitiveness without undermining security or trust.

Key recommendations:

- **Consolidate regulatory frameworks**: ensure alignment between the rules on data intermediation services under the DGA and B2B data sharing under the Data Act. This would remove duplicative requirements and establish a coherent and practical data-sharing environment whilst ensuring clarity.

- **Extend exemptions to mid-cap companies**: Current SME exemptions under the DGA should be

broadened to include mid-cap firms. Many fast-growing European companies exceed SME thresholds but still face disproportionate compliance burdens, which risks penalizing innovation and scaling in Europe.

- **Reinforce safeguards for trade secrets and security**: Clear and robust guarantees must ensure that companies are not forced to disclose sensitive data or security-relevant information that could expose vulnerabilities. Trust in data sharing requires certainty that confidentiality and cybersecurity will not be compromised. As a consequence, (i) the “Security handbrake” in Article 4.2 of the Data Act should be interpreted as to include any impact on cybersecurity as cyber issues can eventually lead to serious adverse effect on the health, safety or security of natural persons; and (ii) and the trade secrets handbrake should not be limited to a governance process but should amount to a genuine protection”.

Application of AI Act requirements (also with respect to the AI Pact)

The AI Act represents a major step in shaping global standards for trustworthy AI. To ensure workable implementation, the Commission should:

- **Ensure certification capacity**: As many harmonized standards will not be complete until late 2026, a reasonable extension of the application of essential requirements should be considered, conditional on the accreditation of conformity assessment bodies.

- **Support integrated conformity assessments and combined certificates**: Where products simultaneously fall under the AI Act, the Cyber Resilience Act (CRA) or the Machinery Regulation, companies should be able to rely on integrated conformity assessments and combined certificates, which may be issued by competent notified bodies. The European Commission could support the development of a Joint Conformity Assessment Framework integrating the cross-sectional obligations to reduce the burden on manufacturers falling under a multitude of regulatory requirements.

- **Provide harmonized templates** for technical documentation, risk management, and post-market monitoring to enable companies to establish uniform compliance processes.

- **Safeguard proportionality and innovation**: Requirements must focus on areas where they add real value. Broad registration of non-high-risk systems or obligations such as source code disclosure risk undermining innovation and intellectual property without delivering proportional safety or transparency benefits.

In addition, clarity on the interaction with other EU data laws (Data Governance Act, Data Act, Free Flow of Non-Personal Data Regulation, Open Data Directive) is urgently needed. Providers of cloud-based and multi-tenant services face uncertainty over mixed datasets containing personal and non-personal data. The Omnibus should provide explicit guidance on how to treat such datasets to ensure compliance without unnecessary complexity.

For AI specifically:

- **Clear definitions and classifications** are essential, distinguishing between AI, machine learning, and generative AI, with mechanisms for addressing new technologies as they emerge.

- **Sector-specific guidance** should be developed, especially in cybersecurity, where AI is already widely used for anomaly detection and automated risk analysis. Clear boundaries between low- and high-risk use cases will allow protective measures to be focused where they are most needed.

- **Public lists of AI categorizations under the AI Act** would assist European companies in their compliance planning and risk management.

Ultimately, companies require predictable, proportionate, and sector-sensitive obligations. This will enable providers - particularly in security - to continue innovating in AI-driven threat detection while ensuring that high-risk applications are subject to appropriate safeguards.

ePrivacy Directive: rules on cookies and other tracking technologies

The Charter of Trust welcomes the European Commission initiative to streamline the ePrivacy Directive through the Digital Omnibus package. As our Partners also serve millions of consumers directly along with businesses, we bring a dual perspective to this debate – one that reflects both entreprise-scale compliance needs and the expectation of individual users. As such, we encourage the European Commission to ensure that any reform of the ePrivacy framework is future-proof, innovation-friendly and responsive to the realities of both businesses and consumer-facing services.

Electronic identification and trusted services under European Digital Identity Framework

The European Digital Identity Framework has the potential to create a trusted foundation for secure and seamless cross-border digital transactions. To deliver on this ambition, implementation must balance security, interoperability, and industry practicality. The wallet should address the public (G2C, G2B) and the private sector (G2B, B2B)

Key recommendations are mainly focused on the wallet for business (EUBW) and on the use along organization (ODI):

- **Set minimum security standards for the EU Business Wallet (EUBW)**: The EU Business Wallet should meet strong baseline requirements, including end-to-end encryption, multi-factor authentication, and resilience against phishing and malware. At the same time, clarity is needed on whether content entering or leaving the wallet should be inspected or trusted by default, to avoid ambiguity in responsibilities.

- **EUBW** should be designed to be used by new business models such as collaborative condition monitoring, participation in new data spaces and services like Manufacturing-X, and compliance with evolving regulatory frameworks including the Eco-design Sustainable Product Regulation (ESPR). This integration is essential for supporting functionalities such as the Digital Product Passport (DPP), particularly in providing verifiable proof of origin and sustainability attributes

- **Cross-border recognition**: Certified digital identities and trust services must be recognized consistently across the Union, without additional national hurdles. Variations in implementation

should be limited, and worthwhile improvements should be adopted uniformly to safeguard trust and interoperability. We count today round 80.000 companies in the EEA which develop and produce machines for the Industrial IoT (IIoT) market. International standards are key for the ongoing digital transformation in industrial automation and smart factories. Examples are Asset Administration Shell (AAS), Digital Twin (DT) and Attribute Based Access Control (ABAC). The EUBW should follow this mainstream.

- **Industry involvement**: The development of technical standards should involve meaningful contributions from security providers, ensuring that the wallet is secure by design, practical to implement, and scalable across sectors and Member States.

- **EUBW should be used** in the context of the Business Registers Interconnection System (BRIS), to verify registered companies and Legal Person Identification (LPID) in the companies.

Taken together, these measures would strengthen the European Digital Identity Framework as a cornerstone of digital trust, fostering both innovation and resilience across the Single European Market.