

The Future of the EU Digital Framework and the Path to Simplification

The European Commission's [Digital Simplification](#) is the next step in the [EU's Better Regulation programme](#). It aims to rationalize an expanding digital rulebook, covering data protection, cybersecurity, and artificial intelligence by removing overlaps and unnecessary administrative load while keeping measures effective and proportionate.

On 19 November 2025, the European Commission published its Digital Omnibus Package, which forms a concrete expression of the simplification agenda described above. The package proposes targeted amendments to key digital-law instruments with the aim of reducing overlap, harmonising thresholds and reporting obligations, and thereby strengthening legal certainty and implementation efficiency while upholding fundamental protections.

The initiative responds to growing uncertainty created by multiple, parallel instruments. As rules on privacy, data governance, online platforms, and AI have multiplied, stakeholders increasingly struggle to see how the frameworks fit together. Simplification is not deregulation: the goal is coherence, transparency, and efficient implementation, without lowering protections.

According to the European Commission's Better Regulation agenda and accompanying impact assessments, the cumulative administrative burden of recent digital legislation, such as the [GDPR](#), the [Digital Services Act](#), the [Digital Markets Act](#), and the [NIS2 Directive](#), has risen markedly since 2018. [EU impact assessment for NIS 2](#) displays that organisations under NIS2 may increase cybersecurity expenditure by 12-22 %, while [GDPR](#) implementation costs for large firms have exceeded €1 million annually in ongoing compliance. Taken together, findings illustrate a broader trend: the number of EU legal acts governing data, cybersecurity, and digital markets has more than doubled over the past decade, reflecting both the EU's regulatory ambition and the growing complexity of implementation.

The Need for Simplification - Complexity Across the Digital Rulebook

The EU's digital regulatory framework has expanded rapidly, resulting in overlapping instruments that often pursue the same goals through different procedures. In practice, the frameworks outlined impose similar duties, recurring transparency reports, risk assessments, technical documentation, and record-keeping, often in slightly different forms. A single service provider may need to file comparable reports under several regulations or conduct parallel risk analyses using varying methodologies. Meanwhile, national authorities responsible for data protection, cybersecurity, and digital markets may interpret identical issues through distinct procedural frameworks.

The outcome is regulatory duplication that raises compliance costs and erodes legal certainty without strengthening user protection. Simplification should therefore prioritise coherence and predictability rather than deregulation. Clearer boundaries between legal acts and closer coordination among supervisory bodies would allow the EU's digital rulebook to remain comprehensive yet practical and provide enforcement that is consistent, efficient, and future-proof.

Key Component I - ePrivacy and Data Simplification

The intersection between data protection and electronic communications remains one of the most fragmented areas of EU digital regulation. The [ePrivacy Directive \(ePD\)](#) was originally intended to complement the [GDPR](#), but its provisions have been implemented unevenly across Member States. Divergent interpretations of consent, cookies, and on-device data processing have produced inconsistent compliance expectations across the Union. While the Directive's goal of protecting user privacy and communication confidentiality is still essential, its application has not kept pace with technological realities. The main source of uncertainty is [Article 5\(3\)](#), which governs the storage of or access to information on user devices. National transpositions vary widely in defining what qualifies as legitimate technical storage and when consent is required. This has led to a fragmented legal environment and a reliance on consent banners that often fatigue users instead of enabling genuine choice. Simplification should focus on clarifying rather than rewriting the Directive. The

Commission could explicitly confirm that consent is not required when cookies or local storage are essential for security, fraud prevention, or service integrity. It could also differentiate between first-party analytics that measure traffic or functionality and cross-site tracking, provided the data remain anonymous and time-limited. Similarly, contextual advertising based solely on the content being viewed could be treated as a low-risk practice, provided transparency and opt-out options are guaranteed.

Further clarification that cookie banners are unnecessary when no consent is requested would reduce excessive notices while maintaining transparency through accessible privacy information. It should also be made explicit that temporary or technical data exchanges, such as those required for normal network functioning, fall outside the scope of consent requirements. The intention is not to lower safeguards but to apply them with greater consistency across the Union. The ePrivacy framework sits alongside the GDPR and newer data governance instruments, yet its practical interpretation often diverges. Aligning these regimes would replace fragmented enforcement with a single, coherent structure. Legal certainty would increase, compliance would become more predictable, and the digital rulebook would rest on a stable and comprehensible foundation.

Key Component II - Cybersecurity and Reporting Alignment

Cybersecurity regulation in the European Union has expanded significantly through the [NIS2 Directive](#), the [Digital Operational Resilience Act \(DORA\)](#), and several sector-specific laws. Each of these frameworks aims to strengthen resilience, improve risk management, and ensure rapid incident response. However, their coexistence has created complex and sometimes overlapping reporting requirements. The NIS2 [Implementing Act](#) (Articles 3 and 11) defines when an incident qualifies as “significant,” while DORA ([Articles 17-19](#)) imposes additional ICT-related incident notifications on financial entities. [PSD2](#) requires payment-related breaches to be reported to national central banks, and [GDPR Article 33](#) obliges controllers to notify data protection authorities of personal data breaches, creating four separate notification channels for a single event. Organisations active in multiple sectors often need to file similar notifications for the same incident, following different formats, timelines, and points of contact. As a result, the fragmentation complicates crisis management and creates uncertainty about which authority should be notified first. It also imposes parallel documentation duties at a time when companies need to focus on mitigation and recovery. In addition, different reporting thresholds based on service type, number of users affected, or perceived impact have resulted in inconsistent application across Member States. Simplification should aim for procedural coherence rather than lowering standards. A single reporting gateway could allow entities to submit one notification through a central digital platform, which would automatically route information to the relevant national and EU authorities. Common definitions of what qualifies as a “significant incident” across NIS2, DORA, and sectoral frameworks would help reduce ambiguity. Harmonised templates and uniform reporting intervals, such as an initial alert within 24 hours followed by a detailed report within 72 hours, would further improve predictability. Increased coordination between [ENISA](#), the [European Central Bank](#), and national authorities would also strengthen consistency. Cross-referencing across existing reporting regimes could further reduce duplication by ensuring that an incident reported under one framework automatically fulfils equivalent obligations elsewhere. Alignment of thresholds and timelines would help avoid premature or repetitive notifications and allow organisations sufficient time to complete internal investigations before submitting final reports. Joint guidance should clarify how incident-reporting duties under different frameworks relate to one another and when compliance with one set of requirements can satisfy others. Similar fragmentation exists at the intersection of cybersecurity, data protection, and financial regulation. The coexistence of GDPR, NIS2, PSD2, and DORA creates parallel reporting obligations that occupy critical staff time during incidents and delay effective response. A single, coordinated gateway potentially managed through ENISA as a one-stop mechanism could streamline notification processes and support thresholds, definitions, and timelines remain consistent across frameworks. Finally, simplification measures should account for the diversity of digital operators. Large providers manage complex systems, while smaller essential service providers often depend on third-party contractors. Guidance should therefore distinguish between primary and delegated reporting responsibilities, maintaining accountability while avoiding excessive administrative work.

Key Component III - Artificial Intelligence and Regulatory Coherence

The Artificial Intelligence Act establishes a comprehensive framework for the governance of AI systems across the European Union, and its horizontal design represents a major step toward risk-based and proportionate regulation. Yet, its implementation coincides with existing laws such as the GDPR, the Digital Services Act, and the [Product Liability Directive](#), which already contain provisions on transparency, accountability, and risk management. There is a clear need to provide coherence among the instruments to prevent duplication and conflicting interpretations. The [Commission's impact assessment](#) indicates that approximately 5-15% of AI applications would fall under the high-risk category. [Independent mapping](#) suggests a similar order of magnitude, with one enterprise sample finding 18% high-risk use cases. For such systems, the Commission's estimates put technical documentation costs in the range of €20,000-€30,000 per downstream high-risk system, with additional costs possible where a quality management system (QMS) must be implemented according to [the Future Society](#). External conformity-assessment costs vary by sector and scope. Overall, there is material overlap between AI-Act documentation and GDPR risk assessments, but the degree depends on the use case and cannot be reduced to a single percentage. A first area of concern is the overlap in risk assessment and documentation requirements. Providers and deployers of high-risk AI systems must carry out detailed conformity assessments and maintain technical records. Comparable procedures exist under data protection law for high-risk data processing and under the DSA for systemic risk mitigation. Without coordination, organisations may be required to repeat similar exercises in multiple formats for essentially the same objective. The issue extends beyond the AI Act itself. Divergent definitions of “automated decision-making” under the GDPR, the AI Act, and the Platform Work Directive have created parallel compliance obligations that are partially overlapping. For example, risk and impact assessments conducted under data protection rules often duplicate the conformity documentation required for high-risk AI systems. Aligning these concepts and recognising equivalence between procedures would strengthen legal clarity and ensure consistent application across regulatory domains. Transparency obligations raise another challenge. The disclosure of training data, system logic, or performance metrics under the AI Act may conflict with trade secret protections and intellectual property rights. At the same time, broad disclosure requirements risk exposing sensitive data without contributing meaningfully to accountability. The Commission should ensure that transparency remains effective but proportionate, and that disclosure practices are aligned across related legislation. Simplification should prioritise interoperability of compliance tools rather than new legislation. Joint guidance by the [European AI Office](#) and the [European Data Protection Board](#) could define when a single assessment, documentation process, or transparency statement satisfies obligations under several laws. Definitions of automated systems also diverge significantly across instruments, creating uncertainty about which activities fall within each regime. A common interpretative note could clarify the scope of “automated decision-making” and distinguish it from broader AI functions. Alignment of reporting and documentation requirements should likewise balance transparency with the protection of commercially sensitive information and trade secrets, ensuring proportionate disclosure while maintaining accountability. Harmonised templates and shared reporting formats would further support a “prepare once, use many times” approach. Finally, a phased and adaptive implementation model would allow guidance to evolve with technology. As AI systems become more complex, flexible coordination among regulators will be critical to maintain both innovation and accountability.

Key Component IV - Product Compliance and Digitalisation of Procedures

The ongoing digital transition is transforming how products are designed, certified, and placed on the European market. The European Commission's “digital-by-default” approach, reflected in the Omnibus IV and related simplification measures, seeks to modernise conformity assessment and product documentation while maintaining the high safety and consumer protection standards that define the Single Market. At present, manufacturers and importers operate under multiple sectoral frameworks that share common objectives but differ in procedure. Requirements for machinery, low-voltage equipment, medical devices, and digital technologies vary in their formats, submission processes, and documentation storage systems. This lack of harmonisation creates duplication, delays market access, and sustains dependence on paper-based workflows. Digitalisation offers a practical solution. Electronic declarations of conformity, digital product passports, and online documentation can reduce administrative effort, facilitate supervision, and improve

traceability. Interoperable technical standards would allow national authorities to access information seamlessly and coordinate market surveillance across borders. In the consumer electronics sector alone, EU compliance costs are estimated at around [€797 million annually](#), and introducing digital product documentation and labelling could reduce these costs by approximately [15 %](#), equivalent to over [€100 million](#) in annual savings. The data suggest the broader economic potential of shifting toward digital-by-default conformity systems. Yet, paper-based manuals and fragmented national documentation practices remain prevalent, suggesting that the benefits of full digitalisation have not yet been fully realised. Simplification should nonetheless preserve the principles of traceability and accountability. Any transition to digital systems must include robust authentication tools, transparent version control, and guarantees of long-term accessibility. Smaller operators should be supported through accessible and cost-efficient compliance platforms to ensure fair participation in the digital environment. The shift toward digital conformity assessment also creates an opportunity to align procedures across product categories. A unified template for digital declarations, combined with automated data exchange between companies and supervisory authorities, could enhance both efficiency and enforcement consistency. In the long run, the success of this shift will depend on balancing innovation with reliability. The aim is not to dismantle the system that safeguards European consumers, but to adapt it for a new era, one in which product compliance is transparent, verifiable, and fully integrated into the digital Single Market.

Key Component V - Regulatory Overlap, Thresholds, and Procedural Simplification

The European Union's digital framework has become a complex mosaic of obligations. Over the past decade, a growing number of legislative acts have emerged, each addressing the same broad themes of accountability, transparency, and proportionality, but doing so through separate channels. The result is not contradiction so much as congestion: rules layered upon rules, sometimes converging, diverging, and frequently competing for the same space. The clearest illustration lies in transparency reporting. A single online platform may be required to produce an annual report under the Digital Services Act, a further set of disclosures under the Platform-to-Business Regulation ([Article 11\(3\)](#)), and thematic submissions under the Code of Practice on Disinformation. Similar exercises appear in the [Audiovisual Media Services Directive](#) and the [Terrorist Content Online Regulation](#). Each instrument defines its own scope, format, and timing. The outcome is duplication rather than depth: multiple reports, slightly different in design but identical in purpose. Each instrument defines its own scope, format, and timing. The outcome is duplication rather than depth: multiple reports, slightly different in design but identical in purpose. The duplication between the Platform-to-Business Regulation and the Digital Services Act illustrates this trend most clearly. Both frameworks require platforms to maintain complaint-handling systems, explain ranking parameters, and issue annual transparency reports. Consolidating these mechanisms under a single, harmonised structure would improve usability and reduce unnecessary administrative effort. In cases where data are not essential for continuous oversight, a reactive reporting model where authorities may request information as needed could maintain accountability while limiting redundant publication.

The same pattern appears in the use of thresholds to determine who is covered by a rule and how strict the obligations should be. The Digital Markets Act classifies “gatekeepers” by user numbers and turnover; the Digital Services Act defines “very large online platforms” by active-recipient counts; the AI Act and NIS2 Directive apply size and impact criteria to define high-risk or essential entities. The thresholds serve to calibrate risk, yet their differing formulas often produce inconsistent designations. A company may qualify as “systemic” under one law and “medium-risk” under another.

The Commission's simplification agenda has the potential to resolve this maze not by dismantling it, but by making its pieces fit together. A single transparency architecture, drawing on the DSA's existing reporting model, could replace a patchwork of separate schedules. Shared metrics, aligned calendars, and a uniform reporting window, two months after the close of each reference period, would transform disclosure from a compliance exercise into a genuine tool of accountability.

Likewise, harmonising threshold definitions would introduce predictability. Common guidance on how user counts, market share, or systemic reach are calculated could eliminate conflicting classifications and allow regulators to focus on substance rather than arithmetic.

Finally, procedural coordination offers perhaps the most immediate gain. Risk assessments, conformity reviews, or audit reports that meet the standards of one framework could, under defined conditions, be accepted across others. This principle of mutual recognition would encourage regulators to cooperate and would spare operators from repeating identical assessments.

The question is not whether the EU should regulate less, but whether it can regulate smarter.