BUSINESSEUROPE

SIMPLIFYING THE EU DIGITAL RULEBOOK

clarity, simplicity, and agility for competitiveness

WWW.BUSINESSEUROPE.EU

JULY 2025

BUSINESSEUROPE

BUSINESSEUROPE'S CONTRIBUTION TO THE SIMPLIFICATION OF DIGITAL REGULATION IN EUROPE

The European Union has become a global leader in digital legislation. Yet with leadership comes responsibility – not only to regulate, but to ensure that regulation, for example on data, cybersecurity, artificial intelligence, truly empowers. As Europe seeks to strengthen its competitive position in an increasingly interconnected world, it must make rules work – clearly, simply, and predictably.

This document puts forward a series of concrete examples to illustrate where and how **(digital) regulation can and must be simplified** to reduce the burdens that hold back European businesses. We commend the initiative and the momentum of the EU institutions to look into these problems, but the anticipation now is about delivery of tangible results.

At the core of our message lies a simple truth: **complexity is not strength.** The proliferation of rules without proper coordination, impact assessment, or clear entry into force timelines has created unnecessary friction. The business community is thus asking to cut disproportionate and excessive burden for **a smarter, more coherent, and more agile regulatory framework** that treats digital not as a siloed sector, but as a cross-cutting enabler of resilience, innovation, and growth. We caution policymakers not to lose sight of the necessary structural fixes in pursuit of micro-adjustments. Reducing ambiguity of EU digital legislation, strengthening the impact assessments, and ensuring inter-service consultation coherence (including on governance/enforcement, deadlines, interplay) are not just technical improvements – they are preconditions for restoring trust in the regulatory process and enhancing Europe's economic dynamism.

This compilation is intended as a constructive contribution to the current simplification drive. It reflects the real-world experience of businesses facing conflicting, overlapping or unclear rules, legal uncertainty, and fragmented enforcement ultimately leading to excessive compliance costs. We hope simplification becomes a strategic enabler for a **competitive and confident Europe** in the digital decade.

FOR FURTHER INFORMATION

Internal Market Department

Martynas Barysas, Director - m.barysas@businesseurope.eu
Svetlana Stoilova, Senior Adviser - s.stoilova@businesseurope.eu

BUSINESSEUROPE
Av. de Cortenbergh 168 – 1000 Brussels

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
Digital Economy: numerous duplications across EU legal acts and multiple implementation bodies involved, resulting in fragmented implementation, Single Market barriers and offsetting of resources from the major objectives of safety and security of goods and services				
1	**Cybersecurity (NIS2, CER Directive, CRA, GDPR)** (Directive (EU) 2022/2555 ; Directive (EU) 2022/2557 ; Regulation (EU) 2024/2847 ; Regulation (EU) 2016/679	Administrative burdens	• These pieces of legislation inconsistently require entities to report incidents which have or can cause a disruption of the provision of the essential or important service. In a hypothetic situation where a physical intrusion/accident (CER-scope) in an energy sector entity, leads to compromise of data, integrity and authenticity of the service (NIS2-scope), the incident is reportable under those two laws, and if the compromise was a function of a publicly known exploited vulnerability of a product integrated in the system - a report of that is also due under CRA-scope (the entity notifies the manufacturer, which still requires a process and human resources allocation); and if personal data was breached the entity must report under the GDPR. o NIS2 Directive requires Cybersecurity incidents to be notified within 24h and reported with more details 48 hours later (72) to the CSIRT, and vulnerabilities to be reported voluntarily. o Overlap with GDPR (EU) 2016/679: requires data breaches (which can be a result of cybersecurity incident subject to the reporting in NIS2 or in CRA) to be reported in 72h to the data protection authority. o Newly adopted Cyber Resilience Act, introduces reporting obligations of 24h to the competent authorities for an incident and/or vulnerability in a product (again potentially overlapping with a cybersecurity incident NIS2, that can also entail data protection breach, GDPR). • Businesses of all sizes are confused with all the reporting requirements and their potential overlaps or reporting similar information several times to different	• Implementation of the "once-only" principle. • A clear instruction that a report of a significant incident to one of the competent authorities (whenever they do not overlap) is deemed sufficient and compliant with all those rules, should be introduced. • In addition, the interim reports "upon request" by the competent authorities under incidents in the scope of CRA and NIS2 Directive should have the option to be refused by the entity, if there is no capability for an action to be taken by the competent authority to directly help the mitigation of the incident (only want interim report if you know you can act upon the information as a competent authority). • The first step is to conduct a thorough mapping of these requirements and administrative setup with respective competences of the authorities in charge to understand the linkages between them as well as potential risks for inconsistencies, fragmentation and negative effects on dedicated resources. Streamlining and simplifying the requirements of the various regulations should be the next step. Compliance authorities are encouraged to make provision for synergies in the event of overlapping reporting obligations in order to avoid unnecessary financial and administrative burdens and to ensure that the notification process runs smoothly and on time. Notification requirements should therefore be harmonized with regulatory frameworks, and a realistic notification timeframe should be defined, taking into account the operational realities of the entities involved. Perfect synergies between the competent authorities will ensure that exchanges of confidential information between authorities are limited to those cases strictly

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
			bodies. Even if one legislation is addressed to entities (NIS2) and the other to processors and controllers (GDPR), or product manufacturers, some service providers (CRA) these roles may overlap in certain cases: an entity can be a controller/processor; a manufacturer could also be a processor/controller; service provider being entity. All this will cost not only legal fees to understand the obligations, but also human hours to execute the different processes and respond to also ad-hoc requests (as NIS2 and CRA allow for authorities to as companies to give updated information "upon request"). Businesses are afraid that resources inevitably will be diverted from the core mission of the cyber-team, i.e. fixing incident or vulnerability.	necessary to protect the commercial interests of companies. • Clear instructions of what a critical product is must be analysed, taking into account the specifics of various industrial sectors/applications.
2	**Market Surveillance** (Market Surveillance Regulation, GPSR, DSA) Regulation (EU) 2019/1020 ; Regulation (EU) 2023/988 ; Regulation (EU) 2022/2065	Administrative burdens	• Under DSA, users, and trusted flaggers can report illegal product or services (where "illegal" means non-compliant with Union or MS law). Since "unsafe" products (GPSR et al.) would essentially be always "illegal" to be sold at the EU marketplaces (as it is not compliant with safety requirements.), technically there is a big overlap of scope. Hence, if a safety issue with a product is reported by the trusted flagger entity as illegal content, the marketplace must act under the DSA to disable access, but also must notify the trader, and most likely the market surveillance authority (Though we could not really find direct texts pointing at this obligation – does it go without saying if you have actual knowledge, given MSR recital 19 mention that – "hosting service providers should not be held liable as long as they do not have actual knowledge of illegal activity or information and are not aware of the facts or circumstances from which the illegal activity or information is apparent.").	• Clearly defining the scope and leaving no margin for diverse interpretations, i.e., "Unsafe products" will be the products that do not comply with safety requirements under EU or national law, which makes them fall under the definition of "illegal content" in DSA. • Trusted flaggers should also report to the Market Surveillance Authority the relevant unsafe product, in order to enable: a) MSAs to take action, and b) MSAs to instruct the marketplace, whether the product must be removed/disabled access to.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
3	**AI Act & Radio Equipment Directive** Regulation (EU) 2024/1689 ; Directive 2014/53/EU	Administrative burdens Cross-border regulatory barriers	• Under the AI Act, Article 6.1 states that an AI system can become high-risk if it is used as a safety component or is a product itself under sectoral EU legislation and is required to undergo a third-party conformity assessment. This implies that an AI product that benefits from the presumption of conformity granted to it by Harmonised European Standards under respective EU sectoral legislation would allow the product to avoid being classified as high-risk and the costs related to this classification. • However, the Commission under the Radio Equipment Directive believes that the AI system would be high-risk under the AI Act irrespective of the existence or application of harmonised standards. • In the case of the energy sector, AI systems intended to be used as safety components in the management and operation of critical infrastructures are considered "high-risk" per the AI Act's Annex III. 2. Yet due to the lack of specificity under Annex III.2 there is no EU common list of infrastructures considered critical. This leaves their identification at country level, which risks a fragmented interpretation of 'critical infrastructure' under the AI Act. • Moreover, EU Countries must identify critical entities by July 2026 (according to the Resilience of critical infrastructures Directive) while the deadline to comply with high-risk AI systems is August 2026. Therefore, energy companies would only have one month to identify which AI systems will need to be certified as high-risk and apply the extensive AI Act requirements.	• The interpretation of the Commission under the Radio Equipment Directive should be changed not to create a precedent of expanding the scope of the high-risk classification into products that may not warrant additional measures. • A common list of infrastructure considered critical should be identified at EU level and enough time should be given to identified AI systems to be certified.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
4	**Declaration of Conformity and other Documenta-tion** Cyber Resilience Act, AI Act, Radio Equipment Directive Eco-design for Sustainable Products; Regulation (EU) 2024/2847 ; Regulation (EU) 2024/1689 ; Directive 2014/53/EU Regulation (EU) 2024/1781	Administrative burden	• The Eco-Design for Sustainable Products Regulation (ESPR) introduces Digital Product Passport (DPP) service providers, what will be a new economic operator in the EU market; companies can use these services to draw up DPP for their products. At the same time, the forthcoming Toy Safety Regulation is discussing a DPP for toys that includes the Declaration of Conformity (DoC), allowing manufacturers to use the toy's DPP to cover any DoC documentation required under other related, applicable rules, such as the RED for radio-connected toys, for example. In similar vein, the Cyber Resilience Act introduced a simplified Declaration of Conformity, which should include a URL where the comprehensive DoC can be found. • The obligation to maintain backup copies of Digital Product Passports (DPPs) via a DPP service provider—especially to ensure availability in cases such as insolvency—lacks clear economic justification in scenarios involving high-volume, seasonal, or short-lifecycle products (e.g. clothing or consumer goods). In such cases, the sheer number of DPPs and the limited long-term value of individual product records would result in disproportionate storage and energy costs, both for economic operators and for DPP service providers, raising concerns about cost-efficiency and environmental sustainability. Additionally, the DPP service provider would be required to retain all back-up DPPs for insolvent or inactive economic operators without the possibility of compensation, effectively transforming part of its activity into a non-commercial service, which raises concerns given that for-profit DPP SP models are not precluded under the ESPR.	• Amend (if necessary for the lack of another measure) the Cyber Resilience Act (CRA), the AI Act, and the Radio Equipment Directive (RED) to allow for the use of the Digital Product Passport (DPP) as a substitute for the paper-based Declaration of Conformity (DoC). • Delete the obligation under Article 10 (4) to provide a back-up copy of the DPP service provider.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
5	**Definitions** CSA, GPSR, PLD, Data Act, CRA, Machinery Regulation; Free Flow of non-personal data; Open Data Directive (non-exhaustive list) (Regulation (EU) 2019/881; (Regulation (EU) 2023/988; (Directive (EU) 2024/2853; (Regulation (EU) 2023/2854; Regulation (EU) 2024/2847 Regulation (EU) 2023/1230 Directive (EU) 2019/1024	Administrative burdens	• **Definitions**: Inconsistent terminology complicates enforcement, market surveillance, and judicial decision-making. Also, diverging definitions create barriers to innovation and trade, discourage cross-border business operations. ○ For example, General Product Safety Regulation, and the Product Liability Directive have definitions of "product", the Data Act provides a definition of a "connected product"; the Cybersecurity Act has an "ICT product" definition, and the Cyber Resilience Act defines "product with digital elements", etc. and this is only horizontal legislation; the definitions of products in sectoral rules should not be neglected. All these laws are essentially setting requirements for products to be placed on the EU market and apply concurrently. ○ Another example is the inconsistent definitions of "substantial modification" in the AI Act, CRA and Machinery Regulation. ○ In NIS2 the definition of "Risk" is correlated to cybersecurity risk, or security risk (unlike the significant cyber risk in CRA), unlike the risk definitions in AIAct, GPSR; Market Surveillance Regulation. ○ The AI Act, the GDPR and the Platform Work Directive have definitions respectively of "AI system"; "automated individual decision-making"; "automated monitoring and decision-making systems"; whereas the latter (the PWD definition) is redundant as it intersects the GDPR and AI Act provisions. ○ Art. 14(7) of the Cyber Resilience Act (CRA) provides a different definition of "main	• The EU Blue guide is a helpful tool to interpret EU product legislation, but it often transpires that even penholders do not necessarily know about the NLF principles, and the Blue Guide's explanations. More streamlining and clarity could be achieved through: ○ A centralized / domain glossary of standardized terms within the EU legal frameworks. ○ Mandatory cross-referencing of definitions when drafting new legislation. ○ A dedicated task force to review and align existing legislation.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
			establishment" than Art. 26(2) of the NIS2 Directive which does not allow companies to fully benefit from the one-stop-shop principle. ○ In the Free Flow of non-personal data the definition "data" is used for non-personal data; in the Data Governance Act, and Data Act the definition of "data" means all digital representations of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording. In the Open data and Re-use of public sector Data the definition of "document" is used for any content whatever the medium (paper of electronic form as a sound, visual or audiovisual recording); or any part of such content; "dynamic data" means documents in a digital form, subject to frequent or real-time updates etc; "research data" means documents in digital form, other than scientific publications, etc.; "high-value datasets" means documents the re-use of which is associated with important benefits for society, etc.	

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
6	**Cyber security conformity assessment** CSA, NIS2, CRA (Regulation (EU) 2019/881; Directive (EU) 2022/2555; Regulation (EU) 2024/2847)	Administrative burdens	• The Cybersecurity Act (CSA) currently operates in isolation from newly adopted EU cyber legislation, including the NIS2 Directive and the Cyber Resilience Act (CRA). Businesses, particularly SMEs, face uncertainty about how voluntary CSA certification schemes interact with emerging cybersecurity and risk management requirements under CRA and NIS2. • The parallel existence of voluntary certification (CSA), third-party conformity assessments, and self-assessment creates confusion and raises the risk of redundant or misaligned compliance efforts. Although CRA does not currently require mandatory certification for any product category, concerns remain that future delegated acts might introduce such obligations. At present, CRA follows the New Legislative Framework (NLF), which enables the use of proportional conformity assessment modules, including self-assessment for low-risk products.	• Acknowledge CSA certification - when voluntarily obtained and where it demonstrably meets relevant legal obligations - as valid evidence of compliance with overlapping requirements under CRA and NIS2, avoiding unnecessary repetition of assessments or audits. • Retain and reinforce the principle of proportionality in CRA implementation by upholding the NLF approach, ensuring that low-risk products continue to be covered by self-assessment modules, without expanding certification requirements beyond what is strictly necessary. • Allow automatic compliance to RED Delegated Act requirements when complying with CRA. (keep the commitment and withdraw RED Delegated Act once CRA shall apply.)
7	**Transparency and reporting requirements for platforms** Digital Services Act, AI Act, GDPR Regulation (EU) 2022/2065; Regulation (EU) 2024/1689) Regulation (EU) 2016/679;	Overlapping rules Administrative burdens	• Parts of the DSA's requirements for transparency, risk management, and oversight of algorithmic systems for digital platforms overlap with the AI Act's rules for high-risk and generative AI systems, as well as with the GDPR, where the latter is already established in terms of format and delivery of information to users.	• Remove the redundant requirements and align the risk-based approaches of DSA and AI Act (e.g. Article 14 DSA; Article 50 AIA). • Amend the scope from algorithmic system in DSA to AI-system to align definitions with the AI Act and the requirements for transparency, risk management and oversight.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
8	**Data protection and financial crime compliance** GDPR Anti Money Laundering /CFT Regulation (EU) 2016/679; Regulation (EU) 2024/1620)	Administrative burdens	• Varying interpretations of data protection laws stand in the way of implementing financial crime compliance and fraud prevention measures in an effective and efficient manner. • There are different types of data with different rules applying to data sharing for financial crime compliance and fraud prevention purposes. For instance, while it is desirable to share as much information on fraud events as possible (e.g., fraudulent IBANs, location data, behavioural data), some EU and national rules restrict access to and sharing of sensitive data beyond Payment Service Providers (PSPs), notably to protect personal data (GDPR). Some fraud prevention measures may be limited to AML/CFT preventing pro-active sharing of fraud suspicion or fraud events. Yet other actors than Payment Service Providers could also play a key role in preventing fraud from spreading to other stakeholders and countries.	• Align fraud prevention and AML/CFT compliance measures in GDPR guidance or in separate laws that foresee an explicit deviation from the GDPR to improve clarity and ensure financial institutions can respond swiftly and effectively to emerging threats, i.e. not only limited to money laundering offences, but also sanctions avoidance, monetary fraud. • Clarify that as a default option, fraud events data could be shared beyond the Payment Service Providers.
9	**Dark Patterns** GDPR, Digital Service Act, Digital Markets Act, AI Act and the Unfair Commercial Practices Directive (UCPD)	Administrative burdens	• "Dark patterns" duplications and overlaps across various regulations and national transpositions of in particular the UCPD lead to a plethora of inconsistent terminology and requirements on how to deal with one and the same issue essentially. For example: • Recital 32 of the GDPR, clearly describing that consent is an affirmative action, freely given and pre-ticked choices do not constitute freely given consent. • Digital Services Act (DSA) – Article 25 addresses the use of dark patterns on online platforms. • Digital Markets Act (DMA) - Recital 37 prohibits gatekeepers to design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent, which is in conjunction with obligations in Article 25 on data protection by design.	• Do not propose new rules on dark patterns, as the current framework has a broad coverage. • Create a cross-DG taskforce between the Units in DG JUST and DG CNECT responsible for monitoring the implementation of the relevant laws, and include relevant stakeholders.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
	Regulation (EU) 2016/679; Regulation (EU)2022/2065; Regulation (EU) 2022/1925; Regulation (EU) 2024/1689; Directive (EU) 2019/2161)		• Unfair Commercial Practices Directive – Particularly Articles 6 prohibits misleading and unfair commercial behavior that causes or is likely to cause consumer(s) to take a transactional decision that would not have been taken otherwise, • AI Act - Article 5 restricts certain manipulative uses of AI systems.	

10	**Use of algorithms in the workplace**
	
	GDPR
	AI Act
	Platform Work Directive (PWD)
	
	Regulation (EU) 2016/679; Regulation (EU) 2024/1689
		Administrative Burdens
		
		Cross-border regulatory barriers
			• Three different regulations—AI Act, PWD, and GDPR—govern the same task allocation systems with differing logics: safety, fairness, and data privacy.
			• Platforms face overlapping obligations (e.g., multiple impact assessments, transparency reporting to both workers and regulators, documentation under different regimes). This causes legal uncertainty, operational complexity, and innovation disincentives.
			• GDPR already regulates much of what the PWD and AI Act seek to impose (e.g. right to explanation, data minimization, human oversight). However, the PWD introduces parallel rights that duplicate these GDPR obligations and could create interpretive conflict (e.g., stricter bans on biometric checks or data categories already addressed by GDPR).
				• Introduce cross-references between AI Act, GDPR, and PWD based on the once-only principle.
				• Align AI Act requirements with existing GDPR principles and recognize sector-specific regulatory frameworks (like the PWD) to avoid double compliance for similar risk scenarios.
				• The PWD should reference GDPR more explicitly, align terminology, and avoid regulating areas already addressed by GDPR unless a compelling reason exists.
				  ○ Limit prohibitions under article 7
				  ○ Align consultation requirements with the GDPR under article 8
				  ○ Align the right to data portability (article 9 with Article 20 of the GDPR)
				  ○ Align transparency requirements in Article 9 with Article 22 of the GDPR)

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
	Directive (EU) 2024/2831		• Furthermore, as the PWD will be transposed in 27 different ways, very different obligations on the use of algorithms may arise between the EU member states.	○ Limit the scope of Article 10 of PWD to the issue as dealt with Article 22(3) of the GDPR ○ Align the timescales under Article 11 with the GDPR • Establish a unified risk assessment framework acceptable under all three. • Encourage joint guidance from supervisory authorities (EDPB, AI Office, Labour Inspectorates).
11	**Spillover effect after cyber-security vulnerability or incident notification** NIS2 Directive, CRA Directive (EU) 2022/2555 Regulation (EU) 2024/2847 ;		• Art 23(1) of NIS2 and Art 17(4) of CRA points that notification shall not subject the reporting 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.	• Both NIS2 and CRA must include a clarification in the form of targeted amendment that the reporting entity is not liable for damages and spill-over effect that have occurred after the notification to authorities had taken place as the information on (unmitigated) vulnerability or (ongoing) incident is no longer only in the control of the reporting entity.
12	**Delays in transposition– grace period** NIS 2 Directive (EU) 2022/2555	Administrative Burdens Cross-border regulatory barrier	• The transposition of NIS2 is currently not proceeding according to the intended timetable. Some countries are implementing the legislation much earlier than others, which creates an uneven playing field for companies (and affects competitiveness), but most importantly causes fragmentation and lack of legal cross-border clarity for companies in Europe.	• Agree on a common minimum grace period, as most EU Member States have still not implemented the NIS2 framework.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
13	**Realistic implementa-tion deadlines Stop-the-clock** **AI Act GDPR Cybersecurity (CSA, NIS2, CRA)** (Regulation (EU) 2019/881; (Directive (EU) 2022/2555 ; Regulation (EU) 2024/2847 ; Regulation (EU) 2016/679 Regulation (EU) 2024/1689	Administrative Burdens	• Products under the scope of Data Act are going to be part of business and consumer-facing products with digital elements under the Cyber Resilience Act. Manufacturers who now are supposed to be compliant with the Data Act (September 2025) will need to reassess or even potentially redesign their products according to the CRA requirements applicable as of December 2027. Additional uncertainty for the manufacturers' risk assessment of a product under CRA comes from the fact that the Data Act's right to data access and users' authorizations for data access to third party(-ies) is impossible to be known in advance by whom and in what circumstances the product and its data will be used. • Cyber Resilience Act standardisation request accepted by European Standardisation Organisations ESOs have a deadline for adoption which is far too close to the applicability date of the CRA: adopting relevant standards (e.g. how to design, develop and produce a product to ensure a proper level of cybersecurity) in October 2027, when the requirements shall apply from December 2027, leaves no time to manufacturers to properly act and comply. At the same time, the CRA introduces mandatory conformity assessments for "important products" to be placed on the market according to these standards after December,11 2027 • AI Act, the guidelines for High-Risk AI systems are scheduled for February 2026, and the obligations related to this type of systems will apply in August 2026, making it necessary to allow sufficient time for the adaptation of the systems in accordance with the guidelines.	• At first stage, provide a "grace period" for compliance for products overlapping under the Data Act and the Cyber Resilience Act, as the product risk assessment of the latter and the subsequent choice of security requirements for the product to be placed on the market may require product design choices that would impact the compliance with the Data Act requirements for data sharing. • Provide manufacturers with reasonable transition allowing for derogations and extended timeframes based on cost benefit assessments. For inspiration see The Energy Performance of Building Directive (EU) 1257/2022 Article 5 and the Directive on Accessibility (EU) 2019/882 Article 14 on disproportionate burden. • In CRA an extended transition period of 36 months is necessary only for product categories whose vertical standards are not ready and harmonised in time (i.e., until December 11, 2027). This would benefit the entire ecosystem by providing companies and national authorities with the necessary time to prepare and adapt to the new regulations. "Stop the clock" mechanism until the relevant standards are being adopted. • Assess other potential grace periods as products under Data Act will make part of the products and services used on site for NIS2 entities, which will also have to comply with CRA obligations for minimisation of vulnerability surface, among others. • Provide a "grace period" for implementing the General Purpose AI (GPAI) Code of Practice • Extend the Implementation Deadlines for AI Act Annex I and Annex III by at least 24 months.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
14	**NIS2 – supply chain** Directive (EU) 2022/2555	Excessive compliance cost	• With the entry into force of DORA since January 2025, as well as with the ongoing national implementation of NIS2, it can be expected that regulated entities will launch detailed verification processes. • Currently, each entity performs this activity using its own templates and interpretations. In practice, this is done in a questionnaire-based format, where different forms with different content are exchanged between entities, requiring a case-by-case approach. This is extremely labor-intensive and at the same time not very productive in terms of ICT asset protection. • Additionally, the recipients of those questionnaires may be an SME, eventually being faced with multiple versions of questionnaires by multiple partners with whom they have contractual relations.	• Develop voluntary harmonised templates for supply chain examination under the various cyber security regulations.
15	**Trade secrets handbrake** Data Act Trade Secrets Directive Regulation (EU) 2023/2854 Directive (EU) 2016/943)		• Manufacturers can be forced to share sensitive data, trade secrets and intellectual property with competitors (and this is not sufficiently balanced even in upcoming model contractual terms from the EU Commission) • Data sharing could raise cybersecurity issues as some data reflect vulnerabilities, and this data must be shared with third parties that may not present sufficient guarantees in terms of security.	Reinforce the security and trade secrets handbrakes by • (i) not limiting the trade secrets handbrake to a governance process but to a genuine protection; and • (ii) expanding the security hand brake to include cybersecurity issues.
16	**Shop online like a local** Geoblocking Regulation (EU) 2018/302	Cross border barriers Administrative burden	• Under Geoblocking Regulation, operators should provide consumers the experience to "shop online like a local", i.e. and asks platforms to maintain the different online interfaces of the website or app accessible from anywhere anytime.	• Launch a cost/benefit analysis considering the current number of customers buying cross-border vs the cost to maintain this number of adjustments.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
17	**Reporting requirements** Gigabit Infrastructure Act Art. 7 (GIA) Regulation (EU) 2024/1309	Administrative burdens	• Reporting requirements in excess, with risk of duplication of work by sending the same information to different areas of the same body, potential errors in data interpretation, and subsequent requests for clarifications and explanations on the information already sent.	• Reduce the statistical information requirements formulated by the different public administrations. • Higher level of coordination/ cooperation between the different Public Administrations or between chambers/ departments of the same administration (e.g. between statistics and competition chamber etc.), and greater sharing of data collected from the different agents, in order to verify (before issuing an information injunction, whether any of their chambers/ departments/ units already have the necessary information for their analysis and objectives. • Consider the feasibility of the Once Only Technical System of the EU for data exchanges between authorities. • Reduce the frequency of remission of information.
18	**Specialised Services** Open internet access Regulation (EU) 2015/ 2120:	Administrative burdens	• Current definition of specialized services: Article 3(5) leave a lot of room for regulatory interpretation, creating considerable uncertainty as to what the regulator will consider as such.	• Provide a non-exhaustive whitelist of services to be considered as specialised services.
19	**Electronic communica-tion networks and Taxonomy** (Commission Delegated Regulation 2022/1214)	Administrative burdens	• Taxonomy-eligible economic activity should include as eligible activity the Provision of electronic communication networks and services	• Inclusion of electronic communication networks (ECNs) as a new Taxonomy-eligible economic activity in the next review of the Climate Delegated Act.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
20	**Data Sharing** FIDA (Proposal for a Regulation on a framework for financial data access) Data Act Regulation (EU) 2023/2854	Administrative burdens	• The new FIDA regulation, currently under negotiation, would impose a significant burden on financial institutions by requiring them to develop data-sharing mechanisms for a very wide range of data, despite a lack of clear use cases and market demand, making cost-benefit justification difficult • Additionally, the interplay and overlap between data user under FIDA and third party/data recipient under Data Act is unclear, as well as other data sharing modalities such as legal restrictions under FIDA for the latter and restrictions under Data Act.	• The impact of the FIDA regulation should be reassessed through the lens of simplification, and it should be significantly adjusted by narrowing its scope and making data sharing conditional on sufficient market demand, • Or withdraw the FIDA Proposal and await Data Act's impact on the sector.
21	**Horizontal vs Vertical Cyber Requirements** NIS2 Directive, Part-IS (Directive (EU) 2022/2555 Implementing Regulation (EU) 2023/203)	Administrative burdens	Aerospace companies must comply with two sets of cybersecurity requirements: the Directive on measures for a high common level of cybersecurity (NIS 2 – horizontal) and EASA's Information Security Regulation (Part-IS – vertical). The application of NIS 2 to regulated industries such as aerospace adds further complexity in the regulatory oversight. Aerospace companies are already subject to specific and much more detailed and comprehensive rules, including on cybersecurity, overseen by EASA, due to the implications on aviation safety.	• NIS 2 requirements should be limited to the applicable functions in an organization (e.g., manufacturing related systems) for critical and essential entities. This would reduce potential burden and conflict with other regulations. • Since the adoption of Part-IS as lex specialis is allowable under Art. 4 and recognition of aviation-specific cybersecurity risk management is recommended under Recital (29) of NIS 2, we encourage Member State authorities to recognize Part-IS as lex specialis to NIS 2 and the European Commission and the European Parliament to support this action.
22	**International (non-personal) data access and transfers** Data Act, Data Governance Act	Administrative burdens	• The General Data Protection Regulation Regime for personal data transfers provides for the identification of jurisdictions with which there is an equivalent protection of the fundamental right of data protection, and therefore personal data transfers could take place. The protection of fundamental rights should ensure that safeguards for both personal and non-personal data are in place, as it would be paradoxical for a jurisdiction to	• Delete the corresponding articles i.e. Articles 31 from DGA and 32 from Data Act. • Introduce in the Data Act a clarification that countries considered having equivalent protection under the GDPR would be considered to have an adequate legal framework also for non-personal data transfers.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
	GDPR Regulation (EU) 2016/679 Regulation (EU) 2023/2854 Regulation (EU) 2022/868		offer strong protection for non-personal data while neglecting the rights and privacy of individuals. Therefore, the provisions in Data Governance Act and in Data Act-would be costly for all sizes of companies (data holders, data processing services) to abide by the two parallel regimes (one for personal and mixed data sets, and one for all other data); and additionally, requiring businesses to assess the compatibility of third-country government data access requests with Union or national law imposes a complex and costly legal burden that could de facto lead to data localization and disproportionately affect smaller economic actors, raising concerns of unequal treatment.	
23	**Product life-time, product support periods** Cyber Resilience Act, Ecodesign for Sustainable Products Regulation; Machinery Regulation Regulation (EU) 2024/2847 Regulation (EU) 2024/1781 Regulation (EU) 2023/1230	Administrative burdens	• During the support period of their products with digital elements, manufacturers are obliged to ensure that, where security updates are available, they are disseminated free of charge. Article 13 (8) CRA prescribes to include other relevant Union law when determining the support period of products with digital elements. This can pose significant challenges to manufacturers. Regulations like the Machinery Regulation or the Ecodesign for Sustainable Products Regulation require manufacturers to define the lifetime of products. Many industrial products have physical lifetimes exceeding ten years, while their digital components follow much shorter innovation and support cycles. Requiring cybersecurity support for the entire physical lifetime imposes disproportionate burdens on manufacturers.	• Distinguish between the physical and digital lifetimes of products with digital elements under the Cyber Resilience Act (CRA). o introduce a "digital lifetime" concept, defined and transparently declared by the manufacturer, to allow for risk-based and economically viable support obligations. This would enhance legal certainty, promote sustainable product use, and maintain the competitiveness of Europe's high-tech industry – without compromising the CRA's cybersecurity objectives.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
24	**Data Processing Impact Assessments** Platform Work Directive GDPR Directive (EU) 2024/2831 Regulation (EU) 2016/679	Administrative burdens	• Article 8 of the Platform Work Directive requires a Data Processing Impact Assessment DPIA under Article 35 of the GDPR where algorithmic management tools are used. While the GDPR doesn't require DPIA to be shared publicly, the Platform Work Directive obliges digital labor platforms to proactively disclose DPIAs (which are very technical and complex documents) to platform workers and their representatives, which is de-fact two regimes for the same entity – one DPIA under GDPR and one for PWD's specific instance. The DPIAs will also be looked at by different authorities • Under GDPR (recital 63) data subjects' rights to access information must be balanced with other rights, e.g. intellectual property protection etc. and such balance should not result in refusal to provide information.	• Remove the obligation to provide the DPIA to workers and their representatives; thus, keeping only the obligation under Article 12 of GDPR for transparent information to data subjects.
25	**Annual reports** The P2B Regulation (Regulation (EU) 2019/1150)	Administrative burdens	• Under Article 11(3) of the Platform-to-Business (P2B) Regulation, platforms are required to establish an internal complaint-handling system and to publicly report annually on its "functioning and effectiveness." (information to be reported among others is total number of complaints received; average time for resolution; main types of complaints; aggregated outcomes). Users not always go via the complaint handling system, rather than other support channels – whether something is complaint under P2B or request for support still requires manual verification in order to be included in the P2B report, thus increasing the man-hours into this compliance practice; Without questioning the legitimate goal of transparency, there is no evidence that the data reported under P2B is used.	• Delete the obligation of annual report of complaint-handling data; provide for on-demand report when the competent authority requests.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
26	**Everlasting Monitoring and Reporting obligations** Cyber Resilience Act (CRA) Regulation (EU) 2024/2847)	Administrative burdens	• Everlasting Monitoring and Reporting obligations (Article 14, Article 69.3) Unlike the vulnerability management obligations, which expire at the end of the last support period at the latest, the obligations to monitor products and report actively exploited vulnerabilities and severe incidents will be mandatory forever. Furthermore, these monitoring and reporting obligations also apply to existing products launched before the CRA became applicable (cf. Art. 69.3). This represents a disproportionate burden, especially for long-standing market participants with many new and especially many legacy products.	• Monitoring and reporting period should be finite and end, for example, five or ten years after the end of the support period
27	**Critical components identification** CRA, NIS2 (Directive (EU) 2022/2555 Regulation (EU) 2024/2847)	Administrative burdens	• In case of insufficient levels of cybersecurity, under NIS 2 Article 24 paragraph 2 the European Commission is empowered to adopt delegated acts, in accordance with Article 38, to supplement the NIS 2 Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881. This could lead to overlaps with the horizontal requirements under the CRA.	• The CE marking according to CRA should be recognised as a sufficient requirement for ICT products under NIS-2. • Delete the delegation of power Article 24 as it is redundant after CRA application date.

No	EU Legislation	Regulatory burden	Burden description	Suggested improvement
28	**Requirements for affiliated companies, or for business groups** NIS2 Directive; DORA (Directive (EU) 2022/2555 Regulation (EU) 2022/2554	Administrative burdens	• Currently, affiliated companies within a corporate group are treated like independent companies in the open market under NIS2.(Article 22 (5)) - • The management of third parties, subcontractors, and ICT suppliers' provisions across regulations can result burdensome when the IT and cybersecurity function is centralized in a single entity within a corporate group (DORA art 28, 29 y 30; NIS2 23).	• If a company offers services that are regulated under NIS2 Article 22 (5) in conjunction with Implementing Directive 2024/2690 exclusively to affiliated companies within the corporate group, then the company and its services should be exempt from the requirements of NIS2 Article 22 (5) and Implementing Directive 2024/2690. • Provide the possibility of centralized or group management for business groups, and the use of harmonized processes and documentation at a corporate group level
29	**Post-market monitoring** AI Act Regulation (EU) 2024/1689	Administrative burdens	• Art. 72(3) requires providers of high-risk AI systems to follow a specific post-market monitoring plan, the template for which will be issued by the Commission through an implementing act. This approach limits providers' flexibility in developing monitoring plans tailored to their specific AI systems and risk contexts. • Companies should be allowed to develop plans that fit their organizational structure and technologies rather than requiring them to follow a monitoring template.	• Revise Article 72(3) to provide flexibility in post-market monitoring

BUSINESSEUROPE

BusinessEurope is the leading advocate for growth and competitiveness at the European level, standing up for companies across the continent and campaigning on the issues that most influence their performance. A recognised social partner, we speak for enterprises of all sizes in 36 European countries whose national business federations are our direct members.

Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic
Denmark	Denmark	Estonia	Finland	France	Germany
Germany	Greece	Hungary	Iceland	Iceland	Ireland
Italy	Latvia	Lithuania	Luxembourg	Malta	Montenegro
Norway	Poland	Portugal	Rep. of San Marino	Romania	Serbia
Slovak Republic	Slovenia	Spain	Sweden	Switzerland	Switzerland
The Netherlands	Türkiye	Türkiye	Ukraine	Ukraine	United Kingdom

Avenue de Cortenbergh 168
B - 1000 Brussels, Belgium
Tel: +32(0)22376511 / Fax: +32(0)22311445
E-mail: main@businesseurope.eu

WWW.BUSINESSEUROPE.EU

EU Transparency Register 3978240953-79