Simplification Recommendations for the Digital Omnibus

Brussels, 10 October 2025

Why this matters

Europe`s technology industries are confronted with an expanding, and at times inconsistent and unclear, digital regulatory framework.

The announced digital omnibus is an opportunity for a much-needed regulatory simplification, while maintaining high levels of data protection and cybersecurity.

Orgalim, representing Europe's technology industries, recommends EU policymakers to include in the digital omnibus the points listed in this paper.

For Orgalim`s general recommendations on simplification, consult the report on: "Reduce regulatory burden to unleash competitiveness."

Overview

Artificial Intelligence Act

Read more: Orgalim position on the Apply AI Strategy

1. Simplify the current high-risk AI classification

- Delete Article 6(1) and Annex I to avoid automatic classification of AI components as high-risk or;
- Merge Sections A and B of Annex I to apply a flexible, sectoral approach and;
- Clarify the scope of AI-based safety components through targeted legal assessments.

2. Postpone the application of the AI Act for high-risk systems

- Delay the application of high-risk requirements until 12 months after harmonised standards are published.
- Suspend fines temporarily until harmonised standards and guidelines are in place.

3. Clarify roles and responsibilities

- Introduce a defined role for "component AI suppliers" and clarify the responsibilities of a "provider" to distinguish between developers and integrators.
- Recognise the original supplier of AI systems and its shared post-market obligations.

4. Targeted amendments to make the AI Act workable in practice

- Consult Annex I for proposed targeted amendments regarding the AI Act.

Data Policy

Read more: Data Union Strategy: Setting the right framework to speed & scale up the use of industrial data in Europe

1. Data Act: Stop the clock and amend

- Postpone the application of Chapters 2, 3, 4 and 6 to 12 September 2026.
- Make Chapters 2 and 3 voluntary, supporting fair access through model contractual terms.
- Amend Articles 1(8), 4.6–4.8, and 5.9–5.11 to exclude trade secrets from mandatory sharing.
- Targeted amendments are needed to make the Data Act workable in practice. See list in **Annex II** below.

2. GDPR simplification while maintaining strong data protection

- Clarify GDPR's interaction with other laws (Data Act, AI Act) and adopt a risk-based approach.
- The simplification proposed for SMCs in the proposed Omnibus IV is welcome but not sufficient.
- Targeted changes can be made while keeping strong data protection. See recommendations in **Annex III** below.

3. Simplify the Data Governance Act:

- Simplify requirements for the provision of data intermediation services (Article 12). They are costly and burdensome.
- Assess whether a DPP service provider (Article 2.32 ESPR) configures as a data intermediary service provider (Article 2.11 DGA) and, if yes, how Article 12 DGA affects the provision of the DPP service.

Cybersecurity Policy

Read more: Orgalim`s feedback to the review of the Cybersecurity Act (CSA)

1. Resolve overlapping or contradictory cybersecurity requirements

- Include a clause to define lex specialis relationships when provisions overlap.
- Repeal the RED Delegated Act on cybersecurity when the CRA becomes applicable.
- Recognise the use of products that bear a CE mark by NIS2 entities as fulfilling product related requirements of Article 21 of the NIS2.

2. Incident reporting simplification

- Create a one-stop-shop mechanism for incident reporting (NIS2, CRA, GDPR).
- Support the development of a single European reporting platform, in close cooperation with ENISA and national CSIRTs (as provided for in Article 16 of the CRA).
- Clarify that reporting obligations for manufacturers shall be limited to the duration of the support period of the PDEs.

3. Ensure practical implementation of the CRA

- Allow Module A (internal production control) as a conformity assessment procedure for "important products" (Annex III, Class I) until vertical standards are available.
- After publication of vertical standards, allow at least 12 months for implementation.

4. Voluntary Certification Schemes

- Reinforce the voluntary nature of CSA schemes and oppose mandatory use under NIS2 and CRA.
- Mandatory certification contradicts the NLF and sets a negative precedent.

5. ENISA Mandate

- Focus ENISA's efforts on existing responsibilities before expanding its scope.
- Avoid duplication of roles between ENISA, Member States, and EU bodies.

Read more: Reduce regulatory burden to unleash competitiveness

Annex I: Recommended amendments to the AI Act

AI Act Reference	Challenge	Proposed amendment
Article 2(6)	It is unclear for manufacturers whether AI systems used exclusively for the research and development of commercial products fall outside the scope of the AI Act.	Clarify that AI systems used exclusively for the research and development of commercial products are out of scope of the AI Act.
Article 3	The absence of a clear definition for open-source software (OSS) creates ambiguity around the applicability of the AI Act to open-source models.	Provide a legal definition of OSS, ensuring clarity on OSS exceptions. Ensure it is aligned with other digital legislation.
Article 3, Article 2(63)	Under Article 3, companies placing a product that incorporates an AI system on the EU market are treated as the "provider" of that AI system, even when it is acquired from a third party. This places full legal liability and compliance obligations on integrators, who often lack control over model development and access to critical information. Under the current definition of 'General-purpose AI model (GPAI)', it is unclear who bears the responsibility of a model used downstream. The model can be developed by a company and placed on the market before being used as a downstream product, without being modified. In the case of a broader interpretation, that would mean reusing LLMs for a GPAI would deem providers of GPAI (e.g. providers of conversational bots) responsible for unreasonable obligations (especially under Chapter V).	Introducing a defined role for "component AI suppliers" with relevant obligations. Clarify that re-using a GPAI model already available on the market for a downstream system without 'substantially modifying' it, would not classify you as the provider of the GPAI model.
Article 11 & Annex IV	Article 11 and Annex IV require providers to prepare and maintain extensive technical documentation to demonstrate conformity. Commercial AI suppliers, particularly those based outside the EU, frequently withhold this information, making it difficult to conduct assessments or fulfil documentation requirements.	Enable harmonised AI supplier declarations to be reused by integrators under Annex VI. This will reduce redundant assessments by integrators and encourage third party AI developers to undergo voluntary certification knowing that their declarations are legally valid downstream.
Article 25(1)(b)	According to Article 25(1)(b), any substantial modification to the AI system makes the modifier the new provider. Even standard integration actions (e.g. API customisation, UX adaptation) may unintentionally trigger this classification, leading to ambiguity and compliance risk.	Clarifying "provider" responsibilities in Article 25 to distinguish between developers and integrators.
Article 27	Duplication of reporting requirements for the AI Act and the GDPR respectively can pose challenges for industry.	Ensure that the Fundamental Rights Impact Assessment (FRIA) templates are built on the same structure as the Data Protection Impact Assessments (DPIAs). Ensure that the DPIAs can be leveraged to prepare the FRIA. This can be done through guidelines analysing the assessments in comparison.
Article 49(2)	Requiring registration of AI systems listed in Annex III but deemed not high-risk under Article 6(3) imposes unnecessary administrative burdens.	Delete Article 49(2) on registration of AI systems within the scope of Annex III, but considered non-high-risk, as per Article 6(3).

Article 57	Absence of clear timelines for listing and operationalising AI sandboxes limits SME and stakeholder planning.	Require the AI Office to provide a timeline for listing sandboxes, increasing transparency for SMEs and other businesses.
Article 72(3)	Mandating a uniform monitoring plan via implementing acts limits providers' ability to develop their own post-market monitoring frameworks and processes.	Delete Article 72(3) which requires providers to follow a specific post-market monitoring plan, whose framework will be designed by the European Commission in an implementing act, giving providers flexibility in developing their own post-market monitoring plan and activities.
Articles 72 & 73	As per Articles 72 and 73, providers must implement systems for post-market monitoring and serious incident reporting. These tasks may not be achievable without technical insight or ongoing support from the original AI supplier.	To address this, the AI Act should formally recognise the role of the original AI supplier and assign them shared responsibilities for post-market obligations. Enable AI suppliers to report incidents directly and mandate access to diagnostic interfaces (e.g. confidence scores, exception logs, API health). This can support a more feasible compliance process for integrators.
Article 74(13) and Article 92(3)	Granting market surveillance authorities access to source code may lead to data breaches or misuse by malicious actors, if the technical safeguards are lacking.	Remove the possibility for market surveillance authorities to access the source code of an AI system or a GPAI model.
Article 82	Allowing restrictions on compliant AI systems undermines legal certainty for providers.	Delete Article 82 on compliant AI systems which present a risk, as compliance with the AI Act should be sufficient for an AI system to be allowed on the market.
Article 83	Current withdrawal measures apply regardless of whether the provider is willing to comply.	Amend Article 83 on formal non-compliance so that the restrictions or withdrawal measures would only apply if the provider refuses to comply.
Article 91	There are no guarantees to ensure the confidentiality of information shared with authorities, risking leakage of proprietary information.	Add protection for trade secrets, ensuring confidentiality of information obtained from General Purpose AI (GPAI) model providers by the European Commission under Article 78.
Article 111	It is unclear how legacy AI systems and GPAI models already on the market will be treated under the regulation.	Apply the legacy clause (Article 111) to all AI already on the market, including GPAI models. As a best practice, legislation should be forward looking, not retroactive, clearly defining the temporal scope of the Regulation.
Article 111(2)	The use of "significant changes" diverges from terminology used in the NLF.	Change "significant changes" to "substantial modifications" to ensure alignment with NLF definitions (e.g. Machinery Regulation).
Annex VI	Annex VI allows providers to reuse conformity documentation from an original provider, but only if the AI system is not substantially modified and all required information is available. Without contractual obligations mandating cooperation from the original developer, reuse becomes unfeasible in most cases.	Enable integrators to reuse supplier-issued conformity declarations under Annex VI. Provide model contractual clauses for AI procurement, including documentation access and monitoring cooperation.
Articles 72 & 73	As per Articles 72 and 73, providers must implement systems for post-market monitoring and serious incident reporting. These tasks may not be achievable without technical insight or ongoing support from the original AI supplier.	To address this, the AI Act should formally recognise the role of the original AI supplier and assign them shared responsibilities for post-market obligations. Enabling AI suppliers to report incidents directly and mandating access to diagnostic interfaces (e.g. confidence scores, exception logs, API health) would make compliance more feasible for the integrators.

Annex II: Recommended amendments to the Data Act

Data Act reference	Challenge	Proposed amendment
Recital 7	As things stand, insofar as the user is not also the data subject whose data is requested, Article 4.12 and Article 5.7 of the Data Act refer to the fact that there must be a **legal basis for the transfer of personal data** in accordance with Article 6 and, if applicable, Article 9 of GDPR.	The following sentence should be deleted from Recital 7: "*[this regulation] does not create a legal basis for providing access to personal data or for making personal data available to a third party*". In addition, on the GDPR side, the Data Act (and at least data sharing under Article 4.1 and Article 5.1) should be regarded as an authorisation within the meaning of Article 6(1)c of GDPR.
Article 1(8)	Risk of undermining **protection of trade secrets**; the current emphasis solely on IPR without including an explicit safeguard for trade secrets creates legal uncertainty and can adversely affect investment/data sharing.	Alongside IPR protection, add that the Data Act is without prejudice to the protection of trade secrets (as defined in the Trade Secrets Directive 2016/943).
Article 4(6)–(8)	The "**Trade secret handbrake mechanism**" is inadequate as it lacks practical effectiveness; the refusal threshold (economic harm) is unrealistically high; trust and incentives for data-driven design are eroded.	Delete Article 4(6), 4(7), 4(8) to exclude trade secrets from data-sharing obligations.
Article 5(9)–(11)	Inadequate protection for **trade secrets in B2B access requests**; legal uncertainty; legalises the delivery of trade secrets to competitors, contradicting technological sovereignty objectives.	Delete Article 5(9), 5(10), 5(11) to exclude trade secrets from the obligation to share data with third parties.
Article 2(13)	Definition of **data holder** is unclear and circular.	Revise definition to a narrow, clear formulation.
Article 2(22)	Per-unit interpretation of "**placing on the market**" is impractical for products with long development/certification cycles.	Specify that, for certain categories of products, placing on the market is determined at model or type level rather than per individual unit.
Article 4	**Lack of legal basis for data holders** to use/share data for core operational and innovation purposes (diagnostics, safety, R&D, quality).	Establish an explicit right for data holders to use and share generated data even without a contract for diagnostics, R&D, quality assurance/control, and safety, while respecting users' rights and applicable data protection, trade secrets, and IPR laws.
Article 4(2)	Potential **legal conflicts** between safety/security legislation and data-sharing obligations; safety/security must prevail.	Clarify precedence: safety and security legislation must clearly prevail over data-sharing obligations under the Data Act.
Article 7(1)	**SME exemptions are too narrow** (currently covering only micro and small enterprises); the recent proposal on small mid-caps (SMCs) argues for broader relief to reduce bureaucracy and support innovation.	Extend Article 7(1) so that SME-type exemptions also apply to medium-sized companies and small mid-caps.
Article 13(4)–(5)	Overlap with national unfair terms regimes; restricts contractual freedom; "in particular" wording creates uncertainty.	Delete Article 13(4) and (5). Alternatively, delete the words "in particular" in Article 13(4)'s first sentence to improve legal clarity.
Chapter V	Fragmentation and inconsistency across government access frameworks increase the administrative burden.	Set a single reporting point for public-sector data access requests, compatible with similar provisions (including the revised European Statistics Regulation).

Article 15(1)(b)	Scope risks enabling broad, **non-essential data requests** from the public sector.	Delete Article 15(1)(b) to limit mandatory requests to public emergencies only.
Chapter IX / Article 37	**Lack of coordinated supervision**; unclear interplay with DPAs/EDPB increases complexity.	Create an EU-level "One Stop Shop". If not feasible, empower the European Data Innovation Board to coordinate national data coordinators in close cooperation with DPAs/EDPB.
Article 37(10)–(13)	**Administrative overlap with GDPR** increases the compliance burden.	Amend to align with GDPR procedures to reduce overlap and ease compliance.
Article 50	**Risk of de facto retroactivity**; transition clarity needed and link to Article 2(22).	Amend to ensure Chapters 2–4 apply only to products/related services (and related contracts) placed on the market after the Data Act starts applying, without prejudice to the amendment of Article 2(22).
Chapters II–III	**Rigid statutory definitions** of raw data and pre-processed data cannot fit diverse IoT value chains and use cases.	Leave the definition of raw vs pre-processed data in B2B sharing to contracts between the parties, enabling necessary flexibility.

Annex III: Recommended amendments to the GDPR

GDPR issue	Challenge the amendment addresses	Proposed amendment
Applying the GDPR to the training of AI models	Uncertainty around lawful bases, purpose limitation, and thresholds for anonymisation/pseudonymisation create legal ambiguity and compliance barriers for EU AI development.	Clarify how the GDPR applies to AI training and usage, including lawful bases, purpose limitation in model development/reuse, and practical thresholds/tests for anonymisation and pseudonymisation.
Non-personal use of personal data	Some processing is unrelated to the data subject (e.g. industrial measurement data) and faces unnecessary GDPR constraints despite minimal privacy relevance.	Scope out cases where the purpose of processing is unrelated to the data subject and the processor has no means, interest, or intention to engage with the personal data aspect, and dissemination is prevented via technical/organisational measures; in these specific cases, allow processing as non-personal data.
Risk-based approach	Certain obligations are not calibrated to risk; low/no-risk processing faces disproportionate requirements (e.g. information duties, records).	Embed broader risk-based distinctions so that low/no-risk processing is exempted or simplified (reduced information obligations and no record of processing where appropriate), reserving full measures for high-risk processing. *Example of low risk: the staff number of a natural person is stored on a machine which is operated by that person and that number is not processed any further.*
Strengthen and clarify legitimate interest and contract	The balance test for legitimate interest is onerous – especially for SMEs – and unnecessary in low-risk cases.	Clarify and simplify use of legitimate interest (Article 6.1.f); explicitly states that in low-risk scenarios no balance test is required for legitimate interest.
Loosening the interpretation of pseudonymisation	There is uncertainty on when pseudonymisation is sufficient for a third party to process pseudonymised data as non-personal data.	Clarify that where pseudonymised data is transferred to third parties without identifiers, such third parties may process it as non-personal data.

Simplification of documentation requirements	Heavy, overlapping documentation burdens (e.g. transfer impact assessments, Data Protection Impact Assessments, Privacy Impact Assessments, Legitimate Interest Assessments); perceived "more is more" supervisory approach by DPAs.	Reduce amount and overlap of assessments.
Facilitate Codes of Conduct for low-risk use cases (GDPR Article 40)	Creation of Sector Codes of conducts has become too cumbersome (even 2–3 years), slowing scalable solutions for typical low-risk scenarios and interoperability with the Data Act/AI Act.	Accelerate and simplify Article 40 Code of Conduct procedures.
Prior consultation with DPAs leading to certification	Prior DPA consultation for potential high-risk cases lacks predictable, actionable outcomes.	Establish a mechanism whereby prior consultation of DPAs for potential high-risk cases can result in official certification that the proposed activity meets data protection standards; require authorities to evaluate submissions and issue certifications where appropriate.

Annex IV: Recommended amendments to the Cyber Resilience Act

CRA reference	Challenge	Proposed amendment
N/A	Overlapping technical requirements across different legislative frameworks can result in duplicated compliance efforts or even conflicting obligations for manufacturers of products with digital elements (PEDs). For example, remote data processing solutions used in industrial settings (e.g. Remote Vision-Controlled Robotics System) are already covered under the NIS2 Directive and their inclusion in the CRA scope would lead to overlapping obligations.	Where overlapping provisions do not address regulatory gaps, include a clarifying clause to define lex specialis relationships. Such a clause would ensure clarity in cases when horizontal legislation duplicates or conflicts with sector-specific frameworks. Prioritisation is essential to ensure clear definitions of key concepts such as 'product with digital elements', 'safety component', and 'technical documentation', especially since these terms often appear in multiple legislative acts with differing interpretations.
Article 16	The cybersecurity legislative framework is weakened by duplications and inconsistencies related to the reporting of cybersecurity incidents. This leads to inefficient governance, which affects the wider digital legislation and increases administrative burdens for manufacturers.	Design a single European reporting platform, in close cooperation with ENISA and national CSIRTs, as provided for in Article 16 in the CRA. This reporting platform should act as a one-stop-shop notification mechanism which includes clear, step-by-step rules for reporting cyber incidents to a single point of contact. Reporting through the platform shall grant compliance with reporting obligations across NIS2, CRA and GDPR. This mechanism shall enable manufacturers to submit a single report, automatically forwarded to the relevant national authorities. Member States would retain full authority, while ENISA's platform would operate solely as a technical intermediary. Develop a secure and efficient mechanism within this platform to facilitate follow-up communication. A centralised mechanism would allow Competent Authorities to share information.
Article 14	The "early warning notification" for reporting actively exploited vulnerabilities is required within 24 hours from becoming aware of the vulnerability. The notification requires submitting information regarding "the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available"	Remove the requirement to provide information regarding "the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available" from the 24-hour early warning notification of an actively exploited vulnerability. Instead, include the information within the 72-hour actively exploited vulnerability notification.

	This information can be included without adverse impact in the broader vulnerability notification, which is due within 72 hours of the manufacturer becoming aware of the issue. This will ease the reporting burden and allow a timelier "early warning notification".	Align reporting of actively exploited vulnerabilities in terms of format, timeframe, thresholds, channels, definitions, processes with reporting obligations across CRA, NIS2 and GDPR.
Article 13	Currently, it is not clear if reporting obligations persist after the support period of the PDE ends.	Clarify that reporting obligations of manufacturers under Article 14 shall be limited to the duration of the support period of the PDEs.
Article 71	The CRA will apply from 11 December 2027, while reporting obligations on actively exploited vulnerabilities and severe incidents begin earlier on 11 September 2026. As the harmonised standard will only be made available as of 30 August 2026, this creates a significant administrative burden which will especially impact SMEs.	Align the start for applicability of reporting obligations with the CRA applicability date of 11 December 2027.
N/A	There is a risk that manufacturers would face successive hardware migrations within a short timeframe. Protocol updates to comply with the Machinery Regulation (MR) are in place, but potential stricter or additional requirements with the CRA can pose a challenge to implement both within the available timeframe. Misaligned timelines would force manufacturers to adapt their testing processes twice. Alignment to successive harmonised standards over a very short period of time would create an administrative burden.	Align the application date of requirements 1.1.9 and 1.2.1 (f) of the MR with the CRA, i.e. December 2027, to avoid repeated efforts and facilitate implementation. Manufacturers would benefit from reduced complexity, lower costs, and streamlined certification processes.
Article 71	To ensure the effective and practical implementation of the CRA, it is essential that the European Commission, in close cooperation with the European Standardisation Organisations (ESOs), as well as technical experts from industry and civil society, define and agree on realistic, technically sound timelines for the development and delivery of the harmonised European standards under the CRA. The pragmatic alternative solution suggested in the proposed amendment column would safeguard legal certainty and contribute to market continuity without compromising cybersecurity objectives.	We recommend allowing Module A (internal production control) as a conformity assessment procedure for "important products" (Annex III, Class I) until vertical standards are available. The vertical standards referred to are the vertical standards for security requirements relating to properties of PDEs (deliverables 16-41 referring to standardisation request M/606). After formal publication of these vertical standards in the Official Journal of the European Union, manufacturers should have at least 12 months to implement them into their development and production processes.
Article 13(7), Article 31, Article 33(5)	Technical documentation obligations for manufacturers are not proportionate for PDEs which are not categorised as important or critical PDEs.	Extend the option of using a simplified format (as for SMEs under Article 33(5)) for fulfilling technical documentation obligations in the case of PDEs which are not categorised as important or critical PDEs.
Article 13(8)	Many industrial PDEs 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. Article 13 (8) CRA mentions that a manufacturer should determine the support period by also taking into account other relevant Union law when determining the support period of PDEs. This is especially relevant in B2B markets, where duration and conditions of support are typically set by	Under the CRA, the support period should be understood as applying to a product's digital elements rather than automatically extending to its full physical lifetime. Manufacturers may declare a support period that deviates from the physical lifetime which they defined under other Union law. All the other criteria, that manufacturers need to consider when defining the support period (Article 13 (8) remain relevant. The period would still be communicated transparently in the technical documentation and product information. For the duration of the declared period, security updates must be still provided free of charge.

	bilateral contracts to reflect risk, usage context and cost allocation.	
Article 3	The CRA's scope includes inherently benign products with digital elements, such as simple sensors, passive electronic components, or basic switching devices (e.g. analogue-to-digital converters, electric toothbrushes, barcode readers). Although these products pose virtually no cybersecurity risks and are not subject to additional protection measures under the CRA, manufacturers are still required to justify in the technical documentation why certain essential cybersecurity requirements do not apply.	To address this imbalance, we request that the technical documentation for inherently benign products with digital elements is simplified to reflect the virtually non-existent cybersecurity risks for these products.
N/A	The Cyber Security Act (CSA) certification schemes were conceived with the notion that they would be (and remain) voluntary. This voluntary aspect has been already severely limited through Article 24 of the NIS2 Directive, which empowers Member States to make European cybersecurity certification schemes mandatory for particular ICT products, ICT services and ICT processes.	We propose to reinforce the voluntary nature of CSA certification schemes. Article 8 of the CRA states that PDEs with the core functionality of a product deemed "critical" under Annex IV are required to obtain a European cybersecurity certificate. These products need to have an assurance level at least 'substantial' under a European cybersecurity certification scheme. We advise against such mandatory use of the CSA schemes as a way to demonstrate conformity, because it goes against the logic of the conformity assessment under the New Legislative Framework (NLF) as established in Decision No 768/2008/EC and is therefore setting a negative precedent.
N/A	The CRA provides a more comprehensive and horizontal framework for cybersecurity. Running in parallel with the Radio Equipment Directive (2014/53/EU) Delegated Act would duplicate compliance efforts, without additional security benefits. In addition, based on industry's experience, regulatory changes without a transition phase are the most challenging as the development of the product, compliance testing and placing on the market have to be taken into account.	Repeal the Radio Equipment Directive (RED) Delegated Act on cybersecurity when the CRA becomes applicable, particularly for products that fall under the scope of both the CRA and the RED Delegated Act. The related harmonised standards 18031-1/2/3 should be supported by the European Commission in such a way that existing product development processes, the cybersecurity risk assessment and technical documentation can also be leveraged for the CRA.
N/A	It is important to resolve contradictory rules on cybersecurity and ecodesign. Manufacturers must have the ability and legal certainty to prioritise device security updates.	For products falling under both the ESPR and the risk classification of the CRA, formulate the delegated acts of the ESPR to ensure that product functionalities may be restricted (even just temporarily) to close security gaps when needed.
N/A	Given the growing volume of cybersecurity legislation, ENISA plays a critical role in providing guidance, support, and coordination, particularly in relation to the NIS2 Directive and the CRA.	Focus ENISA's efforts on existing responsibilities before expanding its scope. Ensure adequate resourcing to meet the growing technical and operational demands. Avoid duplication of roles between ENISA, Member States, and EU bodies.

Annex IV: Recommended amendments to the NIS2 Directive

NIS2 reference	Challenge	Proposed amendment
N/A	Despite being compliant with the CRA, entities within the scope of NIS2 may still face duplicated product-level checks.	Recognise products that bear a CE mark and therefore fulfil all applicable product regulations and essential cybersecurity requirements, as a sufficient instrument for due diligence in the supply chain. By procuring and

	For example: IoT products in an assembly line that bear the CE marking could be considered compliant with NIS2 requirements.	installing CE-marked network and information systems in line with product-specific cybersecurity regulations (e.g. radio equipment and CRA-compliant PDEs), NIS2 entities shall be able to comply with the product related requirements in Article 21 of the NIS2. This includes hardware, remote data processing solutions and software products.
N/A	The NIS 2 Directive covers both "cloud computing service" providers and "data centre service" providers. Recital 35 notes the significant distinction between data centres that are "part of cloud computing infrastructure" (and covered as part of cloud computing services) and a separate type of "data centre services that are not cloud computing services" (that warrant regulation under a separate category). However, there is an inconsistent interpretation across Member States regarding the cloud infrastructure data centres that form part of distributed networks versus those offering on-premises solutions. This has led to inconsistent national administration, undermining the main establishment principle. While Recital 35 clarifies that an exemption applies when data centre infrastructure is owned by the entity itself, the legal interpretation of "entity" remains unclear in cases where IT services are provided within a corporate group. As a result, internal and outsourced IT services may be treated unequally, creating regulatory disparities.	To avoid this unequal treatment, the NIS2 Directive should be interpreted in a way that reflects the economic realities rather than adhering strictly to the formal legal personality of an entity. Unequal treatment of economic units such as corporate groups and business associations can be avoided by providing a clear definition of the term "provider". Further clarify that "provider" refers to any entity which performs activities and provides services for remuneration to a third party. Linked enterprises or partner enterprises, as defined in Commission Recommendation 2003/361/ (concerning the definition of micro, small and medium-sized enterprises), shall not be considered as third parties.
Article 3(4)	Recital 16 of the NIS2 Directive allows Member States to consider the degree of independence an entity maintains from its partner or linked enterprises (both in terms of the network and information systems it uses and the services it provides) when determining its classification. While the intent is to prevent disproportionate obligations on entities that are part of a group but do not operate as essential or important entities themselves, the current approach leaves this assessment to the discretion of individual Member States, potentially leading to inconsistent application across the EU.	Article 3(4) of the Annex to Commission Recommendation 2003/361/ shall not apply for the purposes of this Directive. When applying Article 6(2) of the Annex to Recommendation 2003/361/EC, Member States should take into account the degree of operational independence an entity maintains from its partner or linked enterprises. In particular, consideration should be given to whether the entity operates independently in terms of the network and information systems it uses and the services it provides.
Annex I(1a)	Companies that feed energy into the power grid using solar panels placed on the roof of an office building can be considered within the scope of application of the NIS2 Directive as energy producers. This classification appears to be a technical oversight in the NIS2 Directive, as it was originally intended to apply to entities generating energy as their main business activity. This misalignment could unintentionally hinder the transition to a sustainable economy by imposing disproportionate regulatory obligations on entities whose core operations are not related to the energy sector. It is important to clarify entities which are non-producers.	Add a provision under Annex I(1a) of the NIS2 Directive to clarify that only essential entities which are energy producers (as defined by Directive (EU) 2019/944, Article 2(38)) should be in scope of the NIS2 Directive, if the activity of producing energy is their main commercial or professional activity.

Annex II (3)	Annex II (3) of the NIS2 Directive does not provide for a restriction of "articles" in the context of Regulation (EC) No 1907/2006 (REACH Regulation). This leads to an undetermined number of European manufacturers being in the scope of point number 3. The reason is that manufacturing of articles means manufacturing of "any man-made object". In principle, all manufacturers of substances, mixtures and articles are subject to Annex II (3) of the NIS2 Directive (unless exempted from application as micro and small enterprises).	Amend the definition of important entity in the sector of manufacturing, production and distribution of chemicals to include importers and exclude "articles." Refer to Regulation (EC) No 1907/2006 as a blueprint: "*Manufacturers and importers as referred to in Article 3, points 9 and 11 of Regulation (EC) No 1907/2006 of the European Parliament and of the Council of substances and mixtures as defined in Article 3 points 1 and 2 of aforementioned Regulation*."
Nr.20 Article 21(5)	Nearly all national transpositions of the Directive interpret the cybersecurity risk-management measures outlined in Article 21(2) differently, often through one or more mandatory or voluntary frameworks (whether custom-built or international). These frameworks frequently exceed the Directive's baseline requirements ("gold-plating"), creating a fragmented compliance landscape. For multinational companies, this results in the need to adhere to multiple frameworks for a single legal obligation and to continuously monitor evolving national requirements, imposing a significant administrative burden.	On 17 October 2024, the European Commission adopted Implementing Regulation (EU) 2024/2690. Article 21(5) should clarify that the implementing regulation may be used by essential and important entities, on a voluntary basis, in order to demonstrate compliance with the cybersecurity risk-management measures referred to in Article 21(5).
Nr.21 Article 23	In the absence of a 'one-stop-shop' mechanism, multinational companies deemed "important entities" are obliged to report a cross-border significant incident multiple times, as part of the early warning notification requirement which must be submitted within 24 hours. The reporting must also be submitted in different languages, depending on the national authority which is notified. This represents a significant burden for affected entities, leading to higher compliance costs.	Amend Article 23 of the NIS2 Directive to allow essential and important entities the option to report significant incidents directly to the designated provider of the Single Reporting Platform (SRP), managed by ENISA, as an alternative means of fulfilling national reporting obligations. The SRP provider, or ENISA, should promptly forward submitted reports to the relevant national CSIRTs. Develop a secure and efficient mechanism within this platform to facilitate follow-up communication. A centralised system would allow Competent Authorities to share information, reducing redundant requests and ensuring consistency in messaging.
Nr.22 Article 26(1)	In the absence of a 'one-stop-shop' mechanism, multinational companies with subsidiaries, partner enterprises, or linked entities across different Member States should be required to register and report separately. Otherwise, there is a risk that the respective company tackles cybersecurity incidents or actively exploited vulnerabilities centrally with the aim to reduce the burden of reporting an incident multiple time. This leads to an unjustifiable exemption of multinational companies from national registration or reporting obligations under the NIS2. This divergence undermines the main establishment principle enshrined in NIS2 and creates a fragmented regulatory environment.	Add an exemption to Article 26(1) to include linked enterprises and partner enterprises. Article 26(1): *(d) linked enterprises and partner enterprises within the meaning of Commission Recommendation 2003/361/EC, if their main establishment is in scope of this Directive and falls under the jurisdiction of a Member State.*
Nr.23 Article 41	There are concerns that inconsistent implementation across Member States may hinder the effective application of the intended simplification measures. It is therefore essential to ensure consistent implementation across Member States.	Within 12 months of the NIS2 Directive's entry into force, Member States shall adopt and publish the necessary measures to comply with the amended Directive and promptly notify the European Commission. These measures shall apply from the day following the end of the 12-month period.

Orgalim represents Europe's technology industries, comprised of 770,000 innovative companies spanning the mechanical engineering, electrical engineering, electronics, ICT and metal technology branches. Together they represent the EU's largest manufacturing sector, generating annual turnover of €2,755 billion, manufacturing one-third of all European exports and providing 11.6 million direct jobs. Orgalim is registered under the European Union Transparency Register – ID number: 20210641335-88.

Orgalim aisbl
Arts 56
Avenue des Arts 56,
1000 Brussels, Belgium

+32 2 206 68 83
secretariat@orgalim.eu
www.orgalim.eu
VAT BE 0414 341 438