EUROCHAMBRES

POSITION ON THE CYBERSECURITY PACKAGE

www.eurochambres.eu

Position on the Cybersecurity Package

The Cybersecurity Package can contribute to a stronger EU cybersecurity framework, but it must do so in a way that preserves legal certainty, proportionality and institutional balance. In particular, the governance of ICT supply chain risks should avoid concentrating overly broad powers in the hands of the Commission and instead rest on clear criteria, robust safeguards and a balanced role for national authorities.

1. Executive summary

Eurochambres sees merit in the Commission's efforts to strengthen the EU's cybersecurity framework, but the package must address several important concerns if it is to support both resilience and competitiveness. The most pressing issue is ICT supply chain governance, where the current approach would give the Commission broad powers over country and supplier designations, risk assessments, mitigation decisions and transition conditions.

Given the potentially far-reaching effects on investment, competition, legal certainty and the functioning of critical sectors, a more balanced framework is needed, based on clear and objectively verifiable criteria, stronger procedural safeguards and a better allocation of responsibilities between the Commission and national authorities. The package should also keep ENISA's role clear and complementary, supporting consistency, coordination and practical implementation without creating additional supervisory layers, reporting interfaces or institutional overlap for businesses. In addition, simplification under NIS2 should deliver greater legal certainty and more proportionate obligations in practice, especially for SMEs and companies facing cumulative compliance pressure across supply chains. In this context, exemptions for SMEs are a welcome step towards a more proportionate and workable framework. Across the package, the ECCF should reduce rather than add compliance burdens, and ransomware reporting should be streamlined instead of creating new reporting obligations.

2. Detailed comments on the proposal

ICT supply chain governance

Eurochambres supports the objective of strengthening Europe's technological sovereignty and reducing strategic dependencies in critical ICT supply chains. Greater resilience, stronger European capacities and a more secure digital infrastructure are essential to the Union's competitiveness, economic security and long-term ability to act autonomously. A more coherent European approach to supplier-related and governance risks can therefore be justified in principle, provided that it is designed in a way that is proportionate, predictable and supportive of the internal market.

Nevertheless, the current design of Title IV *Security of ICT supply chains* raises significant concerns regarding legal certainty, proportionality and institutional balance. The central

concern is the extent of the powers that would be placed in the hands of the Commission, including the ability to designate countries, identify high-risk suppliers, define key ICT assets, determine mitigation measures and set transition conditions through an open-ended implementing process. Decisions of this breadth, with major implications for investment, competition and the functioning of critical sectors, require a more balanced allocation of responsibilities and stronger safeguards. This is particularly important because the criteria used for designations remain broad and, in several respects, difficult to verify objectively, creating a risk that measures with profound market consequences could be shaped by political considerations rather than by a sufficiently transparent and evidence-based risk assessment. At the same time, national cybersecurity and sectoral authorities already have relevant experience and tools to assess supply-chain risks in light of national market conditions and security needs. A redesigned framework should therefore narrow and clearly define the Commission's role, ensure stronger involvement of Member States and competent national authorities, and provide for transparent, robust and objectively verifiable criteria.

This means that decisions on designating countries posing cybersecurity concerns, identifying high-risk suppliers, defining key ICT assets and imposing mitigation measures should not be left to an overly open-ended implementing process. The criteria should be clear, objective and based on evidence. They should not allow suppliers to be excluded mainly because of where they are based, where they are established or the nationality of their management, instead of because of a clearly demonstrated risk. Stronger safeguards are also needed because market operators need confidence that such decisions are not taken on the basis of general suspicion or shifting geopolitical assessments alone. In addition, the framework should build more clearly on the expertise and responsibilities of national authorities, which are often better placed to assess operational realities, market structure and the availability of alternatives. Equally important, affected parties should benefit from effective rights of defence, procedural transparency and meaningful review mechanisms. A predictable and credible risk-governance framework is essential not only for cybersecurity, but also for preserving investment certainty and the rule-based functioning of the internal market.

Eurochambres also considers it essential that any supply-chain restrictions remain targeted and operationally workable. Risk mitigation should focus on genuinely critical key ICT assets and allow for differentiated treatment of components according to their actual function and deployment context. Blanket or insufficiently differentiated bans risk causing unnecessary market disruption, critical supply bottlenecks and the emergence of new technological monopolies. Before phase-out obligations are imposed, the economic and operational impact should be assessed comprehensively, including the availability of alternatives, lifecycle considerations, interoperability constraints, labour and transition costs. Where replacement obligations are ultimately deemed necessary, implementation timelines must be realistic and accompanied, where appropriate, by support measures that preserve the ability of operators to continue investing in resilience, innovation and network modernisation.

The role of ENISA

Eurochambres welcomes the intention to clarify ENISA's role and to strengthen its capacity to support a more coherent implementation of Union cybersecurity legislation. The chamber network sees clear value in a strong advisory and coordination function that helps reduce fragmentation, disseminates practical guidance, and supports convergence in supervisory approaches. At the same time, greater clarity of mandate should not lead to an additional

administrative layer for companies. ENISA's role should therefore remain clearly complementary to that of national competent authorities, with a focus on supporting consistency and practical implementation rather than creating parallel supervisory interfaces for businesses active in more than one Member State.

This is particularly important in relation to cross-border supervision and operational support. The chamber network is concerned that, if not carefully framed, the proposed expansion of ENISA's role could result in additional reporting channels, more audit interfaces, and reduced clarity for companies already navigating a complex regulatory landscape. Any enhanced operational role should therefore be strictly request-driven, closely coordinated with national authorities, and designed around a "one incident, one reporting logic" philosophy. The overall objective should be to streamline interactions for companies, not to multiply them.

It should also be underlined that ENISA must not evolve into a parallel standardisation body. Where technical specifications are needed to support certification or implementation, the primary role of the recognised European Standardisation Organisations should be preserved. ENISA may have a useful role in urgent or highly technical cases, but such interventions should remain exceptional, transparent, and time-limited, with a clear pathway towards subsequent standard-setting by CEN, CENELEC or ETSI. This would help preserve coherence, avoid institutional overlap, and maintain confidence in the European standardisation system.

European Cybersecurity Certification Framework (ECCF)

Eurochambres supports the further development of the European Cybersecurity Certification Framework where it genuinely contributes to simplification, trust and internal market coherence. For the chamber network, the value of the ECCF lies in its potential to offer a workable and recognisable compliance tool that reduces fragmentation between national approaches and between different horizontal and sectoral cybersecurity requirements. This objective would, however, be weakened if certification were to become an additional compliance burden itself. Certification should therefore remain voluntary unless explicitly required under sector-specific legislation, and it should be designed as a practical means of reducing duplication rather than generating parallel audit structures.

In this context, particular importance attaches to the recognition of duly implemented international standards. Many companies have already invested significantly in established certification and compliance systems, including ISO/IEC 27001-based frameworks and other internationally recognised controls. Where those systems deliver equivalent outcomes, the ECCF should build on them instead of requiring businesses to start from scratch under a new European layer. A well-designed framework should create synergies with existing practice, reduce duplicative assessments, and make it easier for companies, especially SMEs and businesses in supply chains to demonstrate compliance in a cost-effective manner.

Eurochambres further considers that the relationship between ECCF schemes and sectoral frameworks such as NIS2, CRA or DORA must be clarified more precisely. If European certificates are to support a presumption of conformity, the corresponding requirements, audit cycles and supervisory expectations should be aligned so that businesses do not face double compliance for the same underlying control objectives. Extension profiles should not become a vehicle for additional national requirements that weaken single market coherence.

Finally, candidate schemes need to be developed through realistic timelines and meaningful stakeholder involvement. Market acceptance, technical feasibility and transparency are preconditions for the success of certification, not optional add-ons.

NIS2 simplification

The objective of simplifying the NIS2 framework and increasing legal certainty for businesses is welcome. Across Europe, companies continue to report that recent amendments affecting the scope of application, the categorisation of entities, the treatment of certain sector-specific activities, and the interaction between compliance and supervision remain difficult to interpret in practice. In many cases, external legal or technical advice is still needed simply to determine whether and how the rules apply. A credible simplification package should therefore deliver a clearer and more predictable framework, with proportionate obligations for businesses whose inclusion may otherwise result more from broad formal criteria than from their actual relevance to systemic resilience.

Proportionality should remain the guiding principle. Changes such as the introduction of a small mid-cap category, the adaptation of the size-cap rule in certain cases, and the removal of some smaller entities from scope can make a meaningful contribution to reducing unnecessary burdens where the cost of compliance is clearly disproportionate to the risk addressed. At the same time, this simplification effort would be undermined if new broad, size-independent categories were added without a narrow and operational definition. Extending the framework horizontally to vaguely defined categories such as strategic dual-use infrastructure operators risks reintroducing legal uncertainty, triggering reassessments by thousands of companies, and placing additional strain on both national authorities and businesses just as implementation is beginning to stabilise.

There is also a strong case for limiting national gold-plating. For businesses operating across borders, divergent national additions to cybersecurity risk-management requirements create cumulative cost, reduce predictability, and weaken the internal market. A more harmonised approach is therefore needed, under which Member States would not introduce stricter or additional obligations as a default response, but only in narrowly justified cases. If simplification is to be credible, it must be felt not only at EU level but also in the way the framework is applied across the 27 Member States.

Simplification should also mean that reporting channels are streamlined in practice, so that companies do not have to notify the same incident repeatedly under different procedures. Greater standardisation of reporting formats and information requirements across the relevant legal instruments would also help reduce unnecessary administrative burden.

SME proportionality and practical implementation

For Eurochambres, the treatment of SMEs is a cross-cutting test of whether the package achieves simplification in practice. The chamber network consistently hears from smaller businesses that cybersecurity obligations do not arise in isolation, but accumulate through direct regulation, customer requirements, certification expectations and supply-chain pressure.

This makes it even more important to ensure that SMEs are not drawn into a de facto mandatory compliance regime through procurement conditions, contractual pass-throughs

or market access expectations that go well beyond the formal legislative text. At the same time, a more risk-based approach to determining which businesses fall within scope would improve proportionality further. Size alone is not always an adequate proxy for criticality. In practice, some companies may face substantial compliance obligations even where their role is not critical from a broader economic or societal perspective. A more targeted framework would better align regulatory effort with actual risk, while avoiding unnecessary burdens for SMEs and other smaller market actors. Proportionality must therefore be reflected not only in the legal scope of the rules, but also in how compliance mechanisms operate across value chains.

Explicit safeguards against gold-plating and more practical SME accommodation are therefore strongly supported. This should include clearer guidance, standardised compliance templates where possible, better alignment with existing widely used standards, and transition periods that reflect the limited administrative and financial capacity of smaller businesses. Where Member States introduce additional national requirements beyond the harmonised baseline, the burden is often felt most acutely by SMEs. Stronger discipline on national additions and a more implementation-oriented support framework can improve both compliance and competitiveness for smaller businesses.

Ransomware

Eurochambres supports efforts to improve situational awareness and operational response to ransomware incidents. However, the chamber network considers that this objective should be pursued primarily through simplification and streamlining of reporting obligations, not through the creation of new layers of reporting. In line with this approach, any ransomware-related reporting requirements should remain strictly limited to what is necessary for cybersecurity purposes and should be aligned with the broader objective of reducing duplication under the digital simplification agenda. The focus should remain on the rapid transmission of relevant technical and operational information that can support incident handling and resilience, while avoiding new obligations that add complexity, create legal uncertainty or deter timely engagement by affected entities.

Against this background, caution is warranted with regard to any obligation to disclose highly sensitive financial details linked to ransomware incidents, such as payment amounts, recipients or channels, unless a clear necessity and an appropriate legal framework are established. The concern is not with the policy objective as such, but with ensuring that NIS2 remains proportionate and does not become a vehicle for additional reporting burdens that go beyond its supervisory purpose. A balanced approach would keep reporting focused, confidential and operationally useful, while remaining fully consistent with the broader commitment to simplify rather than expand compliance obligations.

Eurochambres – the association of European chambers of commerce and industry – represents more than 20 million businesses through its members and a network of 1700 regional and local chambers across Europe. Eurochambres is the leading voice for the broad business community at EU level, building on chambers' strong connections with the grass roots economy and their hands-on support to entrepreneurs. Chambers' member businesses – over 93% of which are SMEs – employ over 120 million people.

Previous positions can be found here: https://bit.ly/ECHPositions

Contact:
Policy Advisor for Digitalisation
Mr Cornelius Knaack, Tel. +32 2 282 08 91, knaack@eurochambres.eu

Eurochambres Communications Manager
Mrs Karen Albuquerque, Tel. +32 2 282 08 72, albuquerque@eurochambres.eu

Eurochambres Media and Communications Manager
Mr Alexander Maurer, Tel. +32 2 282 08 55, maurer@eurochambres.eu

@Eurochambres
@eurochambres.bsky.social
www.eurochambres.eu