Position paper on the Cybersecurity Act 2

FEDIL
The Voice of Luxembourg's Industry

Luxembourg, 12 May 2026

A necessary upgrade of the EU Cybersecurity framework, but not at the expense of competitiveness

Position paper on the Cybersecurity Act 2

FEDIL
The Voice of Luxembourg's Industry

EXECUTIVE SUMMARY

- Strengthening cyber resilience, reinforcing EU-level coordination through ENISA and improving coherence across the EU cybersecurity acquis (notably NIS2, the Cyber Resilience Act and DORA) are legitimate and timely objectives.
- At the same time, cybersecurity regulation must remain fully compatible with Europe's competitiveness agenda and the proper functioning of the Single Market.
- Cyber resilience, technological sovereignty and economic competitiveness are mutually reinforcing objectives and must be pursued together through a proportionate, risk-based and technology-neutral framework.
- Cybersecurity is best achieved through diversification, competition and redundancy in supply chains, rather than through broad supplier restrictions that reduce supplier diversity, increase costs and undermine investment predictability.
- The CSA2 framework must remain proportionate and risk-based, technology-neutral, predictable and legally certain.
- CSA2 should genuinely simplify and align existing obligations across the EU cybersecurity acquis, avoiding additional layers of regulatory complexity that could divert resources away from effective risk reduction.

European Cybersecurity Certification Framework

- Cybersecurity certification is welcomed as a presumption of conformity across EU cybersecurity legislation and as a practical compliance tool for businesses.
- Certification must remain voluntary, risk-based and interoperable with NIS2, the Cyber Resilience Act, DORA and sector-specific frameworks, and must not become a de facto market-access requirement.
- CSA2 should prevent the proliferation of overlapping schemes, ensure realistic timelines for scheme development and maintain meaningful, structured and continuous industry involvement throughout scheme development and implementation.
- Certification should function as a genuine compliance enabler, reducing duplication and administrative burden rather than adding new regulatory layers.

ICT supply chain security and high-risk suppliers

- While addressing non-technical risks and geopolitical dependencies is legitimate, the proposed framework raises serious concerns regarding proportionality, legal certainty and market impact.
- Broad supplier restrictions risk reducing competition, forcing reliance on a limited number of suppliers, increasing costs, creating capacity bottlenecks and delaying network upgrades, without necessarily delivering proportionate security gains.
- Any new restrictive measures must remain evidence-based, transparent and risk-driven, be subject to robust due-process safeguards and thorough impact assessments.
- Exclusion of suppliers should remain a measure of last resort, and priority should be given to targeted mitigation measures.
- Legal certainty is further undermined by insufficient clarity regarding the scope of key ICT assets and by asymmetric transition periods across network types.
- Clear and exhaustive definitions of key ICT assets must be set directly in the regulation, and transition periods must be predictable, technology-neutral and applicable to all network types reflecting operational and investment realities.

Economic impact and compensation

- The broader economic impact of large-scale supplier changes appears to have been underestimated. Preliminary indications from independent European studies point to significantly higher costs than envisaged in the Commission's impact assessment.
- The absence of a financial compensation mechanism is a major shortcoming, given the substantial investments already made by operators in equipment that may need to be phased out for politically driven reasons.
- Appropriate compensation mechanisms are necessary to preserve investment confidence, ensure fair treatment and avoid undermining the economic viability of infrastructure operators.

Governance and ENISA's role

- A stronger and better-resourced ENISA acting as a centre of coordination, expertise and support at EU level, notably through enhanced situational awareness, capacity building and support to Member States is welcomed.
- This reinforcement must remain clearly bounded and technocratic in nature, preserving the institutional balance and national competences and avoiding mandate inflation or excessive prescriptiveness.
- ENISA should not evolve into a de facto regulator or standard-setter; formal standardisation must remain the responsibility of European Standardisation Organisations (ESOs), with ENISA focusing on coordination and facilitation.
- Robust governance, accountability, confidentiality and data-handling safeguards are essential to maintain trust between authorities and industry.

FEDIL calls on EU co-legislators to:

- ensure a proportionate, legally certain and risk-based CSA2 framework,
- preserve competition, diversification and investment predictability in ICT supply chains,
- substantially recalibrate Title IV, including scope clarity and predictable transition periods,
- reassess the economic impact of supplier changes and introduce appropriate compensation mechanisms,
- make cybersecurity certification a practical, voluntary and effective compliance enabler,
- maintain a balanced governance model with a clearly defined and bounded role for ENISA,
- ensure proportionate, fair and predictable enforcement mechanisms.

Position paper on the Cybersecurity Act 2

FEDIL
The Voice of Luxembourg's Industry

I. Introduction and general remarks

The European Commission's proposal to revise the Cybersecurity Act (CSA2) represents a major evolution of the EU cybersecurity framework. FEDIL acknowledges the Commission's objective to strengthen Europe's cyber resilience in a context of heightened geopolitical tensions, escalating cyber threats and growing dependencies in ICT supply chains. The ambition to reinforce ENISA's mandate, modernize the European Cybersecurity Certification Framework (ECCF) and introduce a horizontal framework for ICT supply chain security responds to real and legitimate challenges faced by the Union.

Since the adoption of the Cybersecurity Act in 2019, the cyber threat landscape has significantly deteriorated. Cybercrime has intensified, ransomware attacks have proliferated, and geopolitical tensions have increasingly translated into cyber operations targeting critical infrastructure and ICT supply chains. Against this background, FEDIL welcomes the Commission's intention to improve coherence across the EU cybersecurity acquis, including NIS2, the Cyber Resilience Act (CRA), DORA and sector-specific legislation, as well as its efforts to promote security-by-design, improved situational awareness and more harmonized approaches across the Single Market.

At the same time, cybersecurity regulation must remain fully compatible with Europe's broader competitiveness agenda and the proper functioning of the Single Market. Cyber resilience, technological sovereignty and economic competitiveness are not opposing objectives, and, in our view, cybersecurity is better achieved through diversification and redundancy, not supplier restrictions. They can only be reconciled if the regulatory framework remains proportionate, predictable, technology-neutral and legally certain. Europe cannot strengthen security by weakening legal certainty, restricting suppliers on non-technical grounds that reduce supplier diversity or negatively affect investment predictability. Cybersecurity must be delivered through evidence-based and operationally feasible measures, and the CSA2 should genuinely simplify and align existing obligations rather than add further layers of regulatory complexity that risk diverting resources away from effective risk reduction.

FEDIL therefore supports the replacement of Regulation (EU) 2019/881 with a more comprehensive instrument, provided that strong coherence with existing EU cybersecurity and digital legislation is ensured. Clear, stable and harmonized definitions are essential to avoid divergent interpretations, legal uncertainty and duplication across regulatory frameworks. CSA2 must reinforce the Single Market, not introduce new sources of fragmentation through inconsistent national implementation or overlapping obligations.

From an industrial and operational perspective, however, the proposal raises significant concerns regarding proportionality, governance, legal certainty and economic impact. These concerns are particularly acute with regard to ICT supply chain security, where far-reaching mechanisms could have disruptive consequences for operators, markets and long-term investment planning if not carefully calibrated.

This position reflects the concerns and priorities expressed by FEDIL members, notably from the telecommunications, ICT, manufacturing and critical infrastructure sectors. Luxembourg's economy is highly digitalized and deeply integrated into cross-border value chains. For many FEDIL members operating across borders, cybersecurity is not a theoretical exercise but a core condition for business continuity, long-term investment planning and international competitiveness.

Accordingly, this position paper focuses primarily on the implications of the CSA2 for ICT supply chain security and the framework for high-risk suppliers, while also addressing key cross-cutting issues related to governance, proportionality, legal certainty and stakeholder involvement.

II. European Cybersecurity Certification Framework

Beyond governance and institutional balance, the effectiveness of the CSA2 framework will also depend on the extent to which its compliance tools, first and foremost European Cybersecurity Certification, remain workable, proportionate and supportive of market functioning.

1. Presumption of conformity and regulatory coherence

FEDIL broadly supports the objective of strengthening and streamlining the European Cybersecurity Certification Framework (ECCF). FEDIL strongly supports the recognition of cybersecurity certification as a presumption of conformity with other EU cybersecurity legislation. When properly designed and implemented, certification can serve as a practical tool to demonstrate compliance across multiple regulatory frameworks, thereby reducing duplication, administrative burden and compliance costs for businesses.

At the same time, certification should reduce compliance costs and complexity, not introduce an additional layer of obligations. Several safeguards are therefore necessary to ensure that the framework remains workable, proportionate and supportive of industrial competitiveness. In this respect, CSA2 should actively support simplification and coherence within an already dense regulatory landscape.

FEDIL calls for key safeguards to preserve proportionality and workability.

- Voluntary nature preserved
  Certification must not become a *de facto* market access requirement through procurement practices or regulatory expectations. Public authorities and regulators should not impose mandatory certification through regulatory expectations or public procurement practices unless explicitly required by EU law.
- Effective recognition and operationalization of the presumption of conformity
  Certificates must be effectively and consistently recognized by supervisory authorities across the EU, so that the presumption of conformity operates in practice and provides legal certainty for businesses.
- Avoidance of scheme proliferation
  The proliferation of overlapping certification schemes must be avoided. The ECCF should promote convergence and interoperability with existing sectoral schemes, private certifications and international standards.
- Risk-based assurance levels
  Assurance levels and certification requirements must remain strictly risk-based and proportionate to the intended use, threat environment and sectoral context.
- Alignment with other EU frameworks
  Certification schemes must be interoperable with, and not duplicative of, the Cyber Resilience Act (CRA), NIS2, DORA and other relevant frameworks. CSA2 should contribute to simplification and regulatory coherence rather than adding further complexity.
- Certification as a genuine compliance enabler
  Certification schemes must genuinely simplify compliance, reducing duplication and administrative burden. Certification should function as a true compliance enabler, not as a parallel or additional regulatory layer.

- Extend scheme development timelines
  The 12-month deadline for ENISA scheme development risks undermining stakeholder input and quality. We recommend that differentiated timelines should be established: 12 months for existing frameworks, 18-24 months for new specifications, 24-36 months for novel schemes.

2. Governance and stakeholder engagement

Meaningful, structured and continuous stakeholder engagement is indispensable to ensure that cybersecurity certification schemes are technically sound, operationally feasible and economically sustainable. Industry expertise is essential to prevent misalignment between regulatory requirements and real-world deployment conditions.

Against this background, FEDIL expresses strong concern regarding the removal of structured stakeholder bodies at EU level, such as the Stakeholder Cybersecurity Certification Group (SCCG). To date, such bodies have provided a stable and transparent forum for industry input, ensuring continuity, accountability and technical depth in certification-related discussions.

Replacing permanent stakeholder structures with ad hoc consultations or an annual Certification Assembly risks weakening the quality of technical input, reducing transparency and accountability, and undermining the continuity of stakeholder involvement throughout the policy lifecycle.

FEDIL therefore calls for :

- **Robust, permanent and structured consultation mechanisms** at EU level,
- **Meaningful and continuous industry participation**, including through sector-specific working groups,
- **Ongoing dialogue throughout both the legislative development and implementation phases**.

Such an approach is a necessary condition to ensure that CSA2 remains workable, proportionate and firmly grounded in the realities of diverse national markets and industrial ecosystems.

3. Security objectives and level of prescription

FEDIL shares concerns regarding the growing complexity and prescriptiveness of the CSA2 framework. While the objective of strengthening cybersecurity across the Union is fully supported, Articles 80 and 81 introduce an extensive and highly detailed set of security objectives and scheme elements.

While such ambition is understandable, an excessive level of prescription at legislative level risks limiting flexibility and adaptability over time, reducing the capacity of the framework to respond to evolving technologies and threat landscapes. It also increases the risk of overlap and inconsistency with existing horizontal and sector-specific frameworks, including NIS2, the CRA and other elements of the EU cybersecurity acquis.

FEDIL therefore considers that a more principle-based approach, combined with clear prioritization of security objectives, would better support long-term regulatory stability, innovation and effective implementation. Excessive granularity at legislative level risks undermining regulatory coherence and may ultimately weaken, rather than strengthen, the effectiveness of the EU cybersecurity framework.

III. ICT supply chain security and high-risk suppliers

1. Proportionality and intrusiveness of the proposed framework

This section constitutes FEDIL's primary concern. While securing ICT supply chains is a legitimate and necessary objective, the mechanisms proposed raise serious issues of proportionality, legal certainty and market impact.

FEDIL acknowledges that ICT supply chain security can no longer be addressed solely through technical cybersecurity measures. Geopolitical dependencies, foreign interference and other non-technical risks are now part of the threat landscape, and a coordinated European approach is preferable to fragmented national measures.

However, in its current form, Title IV introduces a far-reaching framework that goes well beyond technical cybersecurity risk management. The proposed ICT supply chain security framework grants the European Commission extensive powers, including the designation of high-risk suppliers and the imposition of mandatory mitigation measures. These mechanisms have the potential to significantly reshape procurement choices, market access and long-term investment decisions across multiple sectors, representing a substantial intrusion into corporate governance and established procurement strategies.

Such an approach also risks undermining existing, industry-led risk management practices and raises concerns regarding the legal basis for delegating politically sensitive decisions through implementing acts.

Without clear and robust safeguards, Title IV risks evolving into a politically driven procurement framework by stealth, rather than a proportionate and evidence-based cybersecurity instrument. If not substantially clarified and recalibrated, the framework risks distorting markets, undermining legal certainty and generating unintended security and economic consequences that could ultimately weaken, rather than strengthen, Europe's digital resilience.

FEDIL therefore stresses that any intervention of this nature must be strictly framed and accompanied by robust safeguards. In particular, **measures affecting ICT supply chains must be based on transparent and evidence-based risk assessments, be subject to due process guarantees, including the right to be heard and the right to appeal, and remain proportionate to the actual risk posed, with exclusion measures used only as a last resort.**

Security objectives must be pursued through predictable, transparent and risk-based measures that preserve trust in the regulatory framework and ensure the proper functioning of the Single Market.

2. High-risk suppliers and market impact

The designation of high-risk suppliers and the associated restrictive measures raise major concerns for FEDIL.

In particular, there is insufficient clarity regarding the criteria, assessment methodologies and decision-making processes underpinning such designations. These uncertainties create a risk of sudden market disruptions, supply shortages and price increases, especially in segments where the availability of viable alternative suppliers is limited in the short to medium term.

From an industrial and operational perspective, FEDIL stresses that cybersecurity and resilience are best achieved through diversified, competitive and resilient supply chains, rather than through broad supplier restrictions. Allowing operators to rely on several suppliers enables effective competition, supports access to the most economically advantageous offers and ensures the best balance between price, quality and security. By contrast, frameworks that artificially restrict the number of eligible suppliers risk reducing competition, forcing operators to rely on a very limited set of suppliers and leading to significantly higher costs and less efficient outcomes than would be achieved in an open and competitive supplier landscape, without necessarily delivering proportionate security gains.

FEDIL further underlines that limiting the pool of available suppliers may also generate significant operational and timing risks. Where only a small number of suppliers are capable of delivering replacement equipment, operators may face capacity constraints, extended delivery timelines and delays in network upgrades or migration projects. Such bottlenecks can negatively affect service continuity, undermine investment predictability and slow down the deployment of critical digital and connectivity infrastructures.

In this context, FEDIL cautions against supplier restrictions based primarily on non-technical considerations that are insufficiently operationalized or not clearly linked to demonstrable cybersecurity risks.

Where risks are identified, priority should be given to targeted and proportionate mitigation measures, such as enhanced transparency obligations, contractual safeguards, and appropriate technical controls and audits, rather than blanket restrictions or prohibitions.

Any restrictive decision must be preceded by a thorough and transparent impact assessment, taking into account, inter alia:

- the economic impact on procurement and deployment costs,
- the actual availability of alternative suppliers,
- the environmental impact of premature equipment replacement,
- investment cycles and potential cascading effects across value chains,
- the implications for service continuity and downstream sectors.

FEDIL also questions the legal basis for delegating such politically sensitive decisions to implementing acts, which may not provide sufficient democratic oversight or legal certainty. Decisions with far-reaching consequences for markets, investments and critical infrastructures require a robust legal foundation, clear procedural safeguards and a high degree of transparency.

3. Legal certainty and definition of scope (key ICT assets)

FEDIL is particularly concerned by the lack of clarity regarding the scope of key ICT assets and affected systems, notably as defined in Annex II.

For electronic communications networks, significant uncertainties remain as to:

- which systems are explicitly included or excluded,
- whether ancillary systems, such as billing, customer management or customer fulfilment systems, fall within scope,
- how potential future extensions of scope through delegated or implementing acts can be anticipated by operators.

Such uncertainty undermines legal predictability, investment planning and compliance strategies, particularly for operators managing long investment cycles and complex infrastructures. Core elements defining the scope of application must therefore be clearly and exhaustively set out in the basic legislative act. Leaving such fundamental definitions to future implementing or delegated acts risks weakening legal certainty and creating regulatory unpredictability.

FEDIL therefore calls for a clear and exhaustive definition of key ICT assets and affected systems directly in the regulation, ensuring that operators can anticipate obligations, plan investments accordingly and implement compliance measures in a predictable and legally secure manner.

4. Transition periods and phasing-out requirements

From both a security and an industrial perspective, investment predictability is a core enabler of effective cybersecurity. Operators can only plan secure, resilient and timely migrations if regulatory obligations, timelines and scope are defined in a clear, stable and predictable manner.

In that sense, FEDIL strongly questions the asymmetric treatment of network types under CSA2. While a clearly defined 36-months phase-out period is foreseen for mobile (5G) networks, transition timelines for fixed and satellite networks are deferred to future implementing acts.

This approach creates unequal treatment, legal uncertainty and regulatory cliff-edge effects. From an industrial and operational perspective, fixed and satellite infrastructures are no less capital-intensive, long-lived or critical than mobile networks. Leaving their transition periods undefined undermines investment planning, contractual stability and effective risk management.

Predictability on transition timelines is a prerequisite for orderly migration, investment security and effective risk management, and a necessary condition to ensure that supply-chain security objectives are achieved without disproportionate economic or operational disruption.

FEDIL therefore calls for :

- Clear, harmonized and technology-neutral transition periods applicable to all network types,
- Transition timelines to be specified directly in the regulation, rather than deferred to future implementing acts,
- Timelines that realistically reflect operational migration constraints, including contractual commitments, equipment lifecycles and the availability of alternative solutions.

5. Economic impact, competition and competitiveness

FEDIL regrets that the proposal does not sufficiently assess the broader economic implications of security of ICT supply chains, including:

- increased procurement costs, reduced supplier diversity,
- supply-chain disruptions, extended delivery timelines,
- increased market concentration,
- cascading impacts on downstream sectors and ultimately on consumers.

In addition, FEDIL notes that independent studies at European level are currently assessing the actual economic impact of large-scale supplier changes. Preliminary indications suggest that the costs associated with equipment replacement and forced supplier transitions may have been significantly underestimated in the Commission's impact assessment. These findings call for caution and support the need for a reassessment of the underlying economic assumptions before far-reaching measures are implemented.

FEDIL further underlines that the proposal does not provide for any financial compensation mechanism, despite the fact that operators have made substantial investments in equipment that may need to be phased out or become unusable as a result of politically driven decisions. Where restrictions are imposed for reasons unrelated to the intrinsic security performance of the equipment, affected operators should not be expected to bear the financial burden alone. FEDIL therefore considers that appropriate compensation mechanisms should be established in order to preserve investment confidence, ensure fair treatment and avoid undermining the economic viability of infrastructure operators.

FEDIL members foresee concrete risks of delayed deployment of digital and connectivity infrastructures, including 5G and fixed networks, as a result of constrained supplier availability, higher costs and regulatory uncertainty.

A resilient ICT supply chain requires not only a high level of security, but also competition, diversification and predictability. Cybersecurity and competitiveness are mutually reinforcing only if regulatory measures remain balanced, realistic and proportionate, and are grounded in market and operational realities.

FEDIL therefore calls for a framework that strengthens Europe's security without weakening its industrial base. Measures that undermine supplier diversity, investment capacity or market dynamics risk ultimately undermining the very resilience and security objectives that CSA2 seeks to achieve.

IV. ENISA mandate

1. Governance, institutional balance and national competences

FEDIL recognizes the need to reinforce ENISA's mandate and resources to reflect its expanded tasks. A well-functioning ENISA can provide real added value in terms of coordination, expertise and capacity building at EU level.

Nevertheless, this reinforcement must remain clearly bounded and technocratic in nature. Strengthening ENISA should enhance coordination and consistency across the Union without altering the institutional balance or displacing national competences.

FEDIL therefore calls for :

- **A governance model based on coordination and mutual reinforcement of EU and national authorities**, rather than substitution,
- **Clear prioritization of ENISA's tasks**, to avoid mandate inflation, excessive prescriptiveness and dilution of effectiveness,
- **Robust safeguards to ensure that ENISA does not evolve into a de facto regulator or norm-setter**, beyond its support, coordination and advisory role.

In particular :

- ENISA's role should complement, not replace or override, national authorities' competences,
- Clear governance structures and accountability mechanisms are needed to prevent concentration of powers at EU level and mission creep,
- ENISA's assessments and opinions should remain non-binding and should not predetermine politically sensitive decisions.

Maintaining national sovereignty and operational flexibility is essential, in particular for sectors operating critical infrastructures.

2. Scope of the mandate and task prioritization

FEDIL supports the enlargement of ENISA's mandate to provide increased assistance, capacity building and situational awareness. FEDIL welcomes enhanced support for Member States under NIS2, threat intelligence sharing, the creation of a ransomware helpdesk and the development of a vulnerability management ecosystem.

At the same time, the expansion of ENISA's tasks must be accompanied by clear and disciplined prioritization, to ensure that the Agency focuses on activities where EU-level coordination delivers genuine added value, rather than duplicating or displacing existing national or sector-specific structures.

Against this background, FEDIL calls for:

- Clear prioritization of ENISA's mandate, focusing on tasks where EU-level action demonstrably enhances effectiveness and coherence,
- A strict focus on high-value coordination, support and capacity-building functions, avoiding overlap with existing national authorities, sectoral bodies or established operational frameworks.

3. Standardisation and role vis-à-vis ESOs

FEDIL is particularly concerned about proposals that would expand ENISA's role in drafting technical specifications, as this would represent a significant departure from ENISA's current supporting role vis-à-vis European Standardization Organizations (ESOs). Such a shift would blur established responsibilities within the EU standardization system and risk undermining its effectiveness.

Maintaining a clear and balanced division of responsibilities is essential to preserve the legitimacy, technical quality and industry trust underpinning European standards. The established role of ESOs, based on consensus-driven and industry-led processes, remains a cornerstone of a credible and trusted EU standardization framework.

Against this background, FEDIL calls for:

- The preservation of formal standardization as the responsibility of European Standardization Organizations (ESOs), which operate through established, consensus-based and industry-driven processes,
- A role for ENISA focused on coordination, facilitation and support of standardization activities, without competing with or replacing ESOs.

4. Resources, data handling and trust

While FEDIL welcomes the proposed increase in ENISA's budget and staff, additional resources must be accompanied by clear task prioritization as well as robust governance and accountability mechanisms to ensure effective and focused use of expanded capacities.

FEDIL also notes that ENISA will increasingly handle sensitive business information, including vulnerability disclosures and ransomware incident data. Protecting such information is a prerequisite for maintaining trust and ensuring effective cooperation between ENISA, national authorities and industry.

FEDIL calls for:

- Robust vetting procedures to ensure the integrity and reliability of staff handling sensitive information,
- Strict confidentiality and data protection safeguards governing the collection, processing and storage of sensitive business data,
- Clear limitations on the use and dissemination of sensitive information, to prevent misuse and preserve industry trust.

V. Sanctions and enforcement

FEDIL shares the objective of ensuring effective enforcement of cybersecurity obligations across the Union. However, the sanctioning regime proposed under CSA2 raises serious concerns regarding proportionality, legal certainty and fairness.

In particular, FEDIL is concerned about the level and calibration of penalties, notably administrative fines of up to 7% of global turnover, which risk having disproportionate effects—especially for smaller operators, entities that are part of international groups, and companies operating in smaller markets such as Luxembourg. Such an approach may penalize companies beyond their actual level of responsibility, risk exposure or capacity to influence group-wide compliance decisions and may have a chilling effect on investment and innovation.

Drawing on FEDIL's positions in the context of the Digital Networks Act, enforcement should primarily aim at improving cybersecurity outcomes, rather than imposing punitive sanctions. A progressive, risk-based and corrective enforcement model should be favoured, with a strong emphasis on dialogue, remediation and continuous improvement. Sanctions should therefore remain a measure of last resort, reserved for cases of persistent non-compliance or demonstrable negligence. The framework should clearly distinguish between intentional violations and good-faith implementation challenges arising from legal uncertainty, technical complexity or transitional constraints.

FEDIL therefore calls for a sanctioning regime that ensures:

- Proportionality and predictability, avoiding excessive or automatic penalties,
- Legal certainty and fairness, including clear criteria for the application of sanctions,
- Case-by-case assessment, taking into account the nature and gravity of the infringement, its actual impact on cybersecurity, and the efforts undertaken to mitigate risks and address deficiencies.

Such an approach would strengthen trust in the regulatory framework and foster a culture of compliance and cooperation, rather than defensive or purely formalistic behaviour.

FEDIL
The Voice of Luxembourg's Industry

-.-.-.-.-

About FEDIL

Founded in 1918, FEDIL – The Voice of Luxembourg's Industry is a multisectoral business federation that represents over 750 companies across industry, services, and construction. These members significantly contribute to Luxembourg's economy, accounting for 95% of the nation's industrial production, 75% of private research activity, 25% of national employment, and 35% of the GDP.

As a founding member of BusinessEurope, the European employers' association, FEDIL maintains a dedicated representative office in Brussels to advocate on behalf of its members at the European level.

The federation is also registered in the Luxembourg Chamber of Deputies' transparency register and the EU Transparency Register (number 286194516022-33), underscoring its commitment to transparent and ethical advocacy.

--

FEDIL, the Voice of Luxembourg's Industry
7, rue Alcide de Gasperi
P.O. Box 1304, L-1013 Luxembourg
E.: fedil@fedil.lu – T.: (+352) 435366 -1