Clifford Chance

BRIEFING

EU cyber reforms proposed, including overhauled Cybersecurity Act

2 February 2026

On 20 January 2026, the European Commission proposed a new cybersecurity package intended to strengthen the EU's cybersecurity resilience and capabilities. The package responds to the increasing threat of cyber and hybrid attacks on essential services and democratic institutions. It has two parts: the first proposes to amend and restate the EU's Cybersecurity Act with a new version (Cybersecurity Act 2); and the second to amend the NIS2 Directive. Key changes are intended to:

- enhance the security of ICT supply chains in NIS2 "highly critical" or "critical" sectors, particularly regarding foreign suppliers with cybersecurity concerns;
- simplify the EU Cybersecurity Certification Framework (ECCF) process, notably by relying solely on technical criteria and excluding any sovereignty-related requirements as far as certification is concerned. Certification will give rise to a presumption of conformity with requirements under relevant legislation;
- improve coordination between EU Member States and EU-level actors and support ENISA to act as a central coordinator, including during major cyber incidents, sharing cyber threat intelligence, and vetting suppliers of critical technology; and
- complement revisions proposed under the EU Digital Simplification Package (**Digital Omnibus**), including the single-entry point for reporting and the simplification and clarification of the NIS2 regime.

Action points for businesses

1. If you operate in an NIS2 "highly critical" or "critical" sector, start reviewing your ICT supply chain, including in the light of the risk of suppliers being designated as High-Risk Suppliers. Whilst it is too early to implement operational changes at this stage, are you able to

migrate to alternative providers within a reasonable timeframe if required?

2. Monitor upcoming developments of the Cybersecurity Act 2, including changes concerning the proposed non-technical risk criteria used to identify High-Risk Suppliers.
3. Prepare for heightened regulatory exposure. Expect new legal, contractual and reputational risk where you or members of your ICT supply chain operate in countries that the European Commission considers high-risk.
4. Plan for centralised engagement with ENISA rather than separate Computer Security Incident Response Teams (CSIRTs) in each relevant EU Member State.
5. If your customers are regulated by NIS2, prepare talking points in anticipation of customer queries about your company's exposure to High-Risk Supplier designation.
6. As schemes emerge, revisit whether ECCF certification offers you a way to demonstrate compliance with EU cybersecurity laws. You may need to refresh how secure-by-design principles are embedded into DevOps processes.
7. In 2026, geopolitics is irretrievably linked to cybersecurity. Cybersecurity is not just about technical measures or human error. That has implications for how you think about cybersecurity in your organisation. Do you have the right expertise at the table?

SUMMARY OF KEY CHANGES

Enhancing the security of ICT supply chains

Scope and objective

The proposal introduces a new framework governing security of the ICT supply chains of entities operating in an NIS2 "highly critical" sector (such as banking, cloud services, telecommunications, data centres, energy, transport or public administration) or an NIS2 "critical" sector (such as manufacturing, online marketplaces or social networks).

The framework notably focuses on 'non-technical risk' – including the possibility that a supplier could be subject to 'influence' by a non-EEA government in a manner that undermines service continuity, compromises data security (including through espionage), or affects the integrity of the products or services provided.

The Cybersecurity Act 2 proposal also seeks to align its territorial scope with that of NIS2, under which covered entities are supervised by the EU Member State in which they are established. For cloud providers, DNS providers, data centre providers, content delivery network providers, online marketplaces, search engines, social networks, managed service providers and managed security service providers, the applicable law and competent authority will be those where the entity has its main establishment.

New concepts

The Cybersecurity Act 2 proposes that the European Commission will identify "Key ICT Assets", being assets that perform essential or sensitive functions. Incidents affecting Key ICT Assets could cause serious disruption to ICT supply chains. The designation of Key ICT Assets will be based on a cyber risk assessment conducted at an EU level.

It is also proposed that the European Commission will designate "High-Risk Suppliers", being suppliers from countries that pose a high risk to EU security based on their law, legal system, practices and/or evidence of malicious cyber activity being conducted from them. High-Risk Suppliers are proposed to be barred from participation in public procurement for ICT components linked to key ICT assets, EU cybersecurity certification and conformity-assessment functions, and the provision of ICT components for Key ICT Assets, among other things.

A framework for centralised intervention

The Cybersecurity Act 2 envisages that the European Commission will be able to: (a) prohibit categories of NIS2 entities from using, installing or integrating ICT components from High-Risk Suppliers into Key ICT Assets; and (b) require categories of NIS2 entities to implement certain mitigation measures, which might include supplier transparency obligations, restrictions on transfers or remote processing from a foreign country, a requirement to submit to a third-party audit of technical safeguards, a limit on the ability to outsource, the imposition of vetting requirements on personnel, or a direction to diversify an ICT supply chain. Infringing European Commission prohibitions or mitigation measures can lead to penalties of up to 7% of global annual turnover for the most serious violations.

Note: By way of comparison, the UK's proposed Cyber Security and Resilience Bill goes further than this. On top of requiring regulated entities to manage cyber risk in their supply chain, the Bill envisages direct regulation of the most critical suppliers.

Telecommunications sector

The Cybersecurity Act 2 proposes to impose more rigid and onerous requirements on mobile, fixed and satellite electronic communications networks. Regulated entities would be required to phase out ICT components from High-Risk Suppliers and must stop using or installing in, or integrating such components into, the operation of Key ICT Assets.

Simplifying the ECCF

Scope

Under the Cybersecurity Act, the ECCF provides a mechanism to attest to compliance with specified security requirements in respect of ICT products, ICT services, and ICT processes. The Cybersecurity Act 2 proposes to extend the mechanism to allow schemes that attest an organisation's broader cybersecurity maturity and readiness (or 'cyber posture'). This means that schemes may become available that allow entities to obtain EU cyber certifications as to their cyber posture. Entities wishing to obtain such certification would need to look at cybersecurity through a wider lens, which may mean taking into account broader factors such as geopolitical

forces and the threat of emerging technologies including AI and quantum cryptanalysis being weaponised by threat actors.

Technical, not sovereignty-based, criteria

Under the proposal, EU certification schemes will rely exclusively on technical criteria. The Cybersecurity Act 2 does not introduce sovereignty-based requirements in the area of certification, such as protection against extraterritorial laws, limits on non-EU ownership, or restrictions on foreign contractors, even at the highest assurance levels. This approach reflects lessons learned from the unsuccessful EU Cloud Certification Scheme (**EUCS**) proposal, which is currently on hold due to disagreements over sovereignty provisions.

Interactions with national schemes

It is proposed that national certification schemes that cover the same subject matter as an EU certification scheme will cease to have effect. For example, if an EU cloud certification scheme akin to EUCS is introduced and adopted, national sovereignty-based schemes – such as France's SecNumCloud – might be discarded.

Quicker development of certification schemes

It is proposed that ENISA will create certification schemes in response to requests from the European Commission. The process of creation would be subject to structured stakeholder involvement and clearer deadlines. ENISA would be held accountable for keeping certification schemes up to date.

As background, EU Member States and industry stakeholders have voiced concerns that the current process for developing and implementing certification schemes is lengthy and ineffective, with only one in every five schemes requested having ever come into force.

A process for technical specifications

The Cybersecurity Act 2 proposes to create a dedicated process for ENISA to draft technical specifications behind certificate schemes, including how they are to be published or, where they contain sensitive information, restricted.

Elevating and empowering ENISA

An expanded role

The Cybersecurity Act 2 seeks to cement ENISA's role as the central hub for European cybersecurity. Specifically, it is proposed that ENISA will:

- issue targeted technical guidance to EU Member States and the European Commission on cyber risk management, maturity assessments, incident response procedures and secure-by-design principles for digital products;
- support EU-level coordinated security risk assessments of critical ICT services, systems and product supply chains;

- develop cybersecurity sandboxes for safer innovation and testing;
- issue early alerts on major or cross-border cyber threats; and
- provide analysis of emerging cyber risks.

New operational functions

The above will be supported by new operational functions. It is proposed that ENISA will:

- maintain the European Vulnerability Database, which will keep track of publicly reported software and hardware vulnerabilities;
- operate the EU Cybersecurity Reserve, being a deployable pool of incident response service providers under the Cyber Solidarity Act;
- coordinate and provide support for cross-border crisis response upon request from the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe);
- operate a ransomware helpdesk to assist essential and important entities in responding to attacks;
- operate the single reporting platform introduced under the Cyber Resilience Act and the proposed single-entry point for incident reporting proposed under the Digital Omnibus;
- support conformity assessment procedures in respect of cybersecurity requirements;
- contribute to European and international standardisation activities; and
- develop workforce capability through EU-wide cybersecurity skills attestation schemes.

Tweaking NIS2

What's in the Digital Omnibus?

On 19 November 2025, the European Commission published the much-anticipated Digital Omnibus, part of which proposed to simplify and consolidate elements of the EU's digital acquis in the areas of data, privacy and cybersecurity. Relevantly, proposed technical changes to NIS2 include creating a single-entry point, taking into account the single reporting platform established under the CRA, for organisations to report cyber incidents in fulfilment of incident-reporting obligations under NIS2, the CER Directive, DORA, the GDPR and eIDAS; and providing that a notification of a severe incident under the CRA constitutes reporting of information under NIS2. The Digital Omnibus proposal is currently making its way through the EU legislative process, which may see aspects of the proposal change.

What's now being proposed?

The January cybersecurity package's proposals include:

- measures to harmonise the substantive obligations in NIS2, by having the European Commission regularly assess the need for EU-wide implementing acts that set out specific measures with which NIS2-regulated entities must comply and preventing EU Member States from adding further measures in addition to those in such implementing acts;
- empowering national CSIRTs to request additional information when a significant incident reported to them is caused by ransomware, including whether a ransom demand was made, by whom, whether it was paid, the amount, the payment method, and certain other particulars about the payment. This information is helpful for collecting intelligence on ransomware, meaning ENISA will be better equipped to support entities in defending against ransomware attacks;
- empowering EU Member States to require entities to obtain EU-wide cyber-posture certification under a yet-to-be-devised scheme. This certification is of an entity's overall cyber-posture rather than the satisfaction of cybersecurity considerations at the product or service level. The certificate might be used to demonstrate compliance with security risk management requirements under NIS2. This should make it possible to use EU-wide certification to show compliance with domestic-level cyber obligations;
- that ENISA will (to a limited extent) facilitate cooperation between national authorities, including by helping to choose a lead supervisory authority for enforcement action involving multiple authorities. ENISA will also prepare a risk analysis on the impact of cyber incidents on entities that operate across borders, in response to which supervisory authorities may then engage in joint activities;
- that "small mid-cap enterprises" (i.e. enterprises with <750 employees and <€150 million in annual turnover) caught by NIS2 are deemed only "important entities" (rather than "critical entities", meaning they are subject to less stringent obligations under NIS2); and
- adjustments to the definitions of sectors in the Annexes to NIS2.

Next steps

Both parts of the cybersecurity package are now expected to progress through the ordinary EU legislative process. We are still at the beginning of that process and the texts are likely to evolve as negotiations advance. The proposals are tied to sensitive and critical tech security, sovereignty, and strategic autonomy issues that are at the heart of current global discussions and concerns.

Once passed into law as a regulation, the Cybersecurity Act 2 is set to apply directly in all EU Member States, subject to adjustment periods for ICT supply-chain rules in implementing legislation. As for the NIS2 adjustments, the proposal contemplates a 12-month transposition period following entry into force of the NIS2 Directive, during which EU Member States will legislate the changes into their domestic law.

The EU's cybersecurity package is part of a broader drive focussed on tech security, sovereignty, and strategic autonomy, with several other initiatives already underway and more on the horizon such as the European Commission's upcoming tech sovereignty package. In parallel, several initiatives are in motion to simplify the EU's cyber (and broader tech)

rulebook, including the Digital Omnibus proposals as well as the Digital Fitness Check.

Businesses will want to closely monitor these important developments, making sense of different parallel objectives and initiatives, assess and ready themselves for their impacts, and consider whether they want to get involved in the discussion, including through consultations.

Authors

Dessislava Savova
Partner, Head of Continental Europe Tech Group, Paris

dessislava.savova@cliffordchance.com
+33 1 4405 5483

Holger Lutz
Partner, Frankfurt

holger.lutz@cliffordchance.com
+49 69 7199 1670

Gregory Sroussi
Counsel, Paris

gregory.sroussi@cliffordchance.com
+33 1 4405 5248

James Wong
Senior Associate, London

james.wong@cliffordchance.com
+44 207006 3750

Alexander Kennedy
Knowledge Director – Tech Group, Europe, Paris

alexander.kennedy@cliffordchance.com
+33 1 4405 5184

Rita Flakoll
Knowledge Director – Tech Group, Global, London

Rita.Flakoll@cliffordchance.com
+44 207006 1826

Other Contacts

Jonathan Kewley
Partner and Co-Chair of the Global Tech Group, London

jonathan.kewley@cliffordchance.com
+44 207006 3629

Anna Carrier
Head of EU Tech Policy, Brussels

anna.carrier@cliffordchance.com
+32 2 533 5048

Andrei Mikes
Counsel, Amsterdam

andrei.mikes@cliffordchance.com
+31 20 711 9507

Patrice Navarro
Partner, Paris

patrice.navarro@cliffordchance.com
+33 1 4405 5371

Herbert Swaniker
Partner, London

herbert.swaniker@cliffordchance.com
+44 207006 6215

Andrea Tuninetti Ferrari
Counsel, Milan

andrea.tuninettiferrari@cliffordchance.com
+39 02 8063 4435