ALLIANCE

Global legal&tax Advisor

CLIENT ALERT EU CYBERSECURITY ACT PROPOSAL

11.03.2026

EU CYBERSECURITY ACT PROPOSAL:

Governance, Resilience, and Market Access

Executive summary

On 20 January 2026, the European Commission presented a comprehensive "*Cybersecurity Package"*, proposing a targeted revision of the "*EU Cybersecurity Act*" (originally adopted as Regulation (EU) n. 2019/881) alongside amendments to Directive (EU) n. 2022/2555 ("**NIS2 Directive**").

The original 2019 framework established a permanent mandate on the "*European Union Agency for Cybersecurity*" ("**ENISA**") as the Union's central technical authority and introduced the "*EU Common Criteria-based"* ("**EUCC**") scheme, laying the foundations of the European cybersecurity certification system.

Since then, the overall set of existing and emerging threats, has evolved considerably. Modern attacks frequently disrupt vital operations and industrial networks, revealing structural flaws in cross-border coordination.

The 2026 proposal arrives at a critical juncture where cyberattacks no longer target data alone, but increasingly jeopardise critical infrastructure, essential services, as well as global supply chains. These vulnerabilities are compounded by hybrid threats and growing geopolitical dependencies on foreign technologies.

Consequently, the proposal moves beyond mere technical standards to address systemic bottlenecks, aiming by reinforcing ENISA's mandate and restructuring the certification architecture to ensure greater uniformity across the internal market. Additionally, it establishes a formal mechanism to manage risks within ICT supply chains, including the identification of high-risk providers and the implementation of safeguards in high-priority sectors.

For businesses, cybersecurity is no longer confined to regulatory compliance. It directly affects market access, contractual stability, investment planning, and long-term competitiveness within the European digital economy.

The proposal will now follow the ordinary legislative procedure before the European Parliament and the Council of the EU, then entering a phase of interinstitutional negotiation and technical refinement. If adopted, it is likely to redefine both regulatory obligations and competitive dynamics within the European digital market.

***

Regulatory standstill and outlook

The proposed reform initiative marks a shift from a predominantly technical compliance regime toward an integrated governance model anchored in institutional consolidation. At its core lies the strengthening of ENISA as the Union's central technical authority.

By formalising the Agency's role in drafting candidate schemes and providing structured technical support to national authorities, the European Commission seeks to eliminate the fragmented national practices that have historically undermined mutual recognition across the EU. This approach ensures a uniform interpretation of assurance levels (ranging from "basic" to "high") while harmonising evaluation methodologies to facilitate a truly smooth internal market.

The expansion of ENISA's mandate includes operating a central EU-wide threat repository, issuing strategic early warnings, managing a unified incident reporting platform, and coordinating large-scale cybersecurity exercises across Member States. These functions position ENISA as the European Union's definitive technical reference body, bridging the gap between high-level policy and real-time operational coordination.

In the meanwhile, the reform seeks to increase the practical relevance of EU certification schemes. Acknowledging that voluntary schemes have had limited adoption, the European Commission is refining procedures and linking certification more closely with other EU product regulations. This strategy eliminates administrative redundancies and prevents the duplication of audit requirements.

Certification development has also been modernised: new procedures incorporate proportionality principles, encourage international cooperation, and set a clear 12-month timeline for ENISA to propose new schemes. By prioritizing global interoperability, the EU intends to reduce compliance burdens for European companies while establishing its certification framework as a leading international standard.

Most significantly, the revision introduces a step change in supply chain security, treating certification as a tool for technological resilience during geopolitical instability. The creation of mechanisms to identify and monitor high-risk suppliers across eighteen critical sectors represents a decisive move against systemic risks. For the first time, the EU framework allows for the potential withdrawal of deployed products if a supplier is reclassified as high-risk, posing operational and financial implications for critical infrastructure and digital services.

Strategic imperatives and the evolution of digital governance

The proposed reform introduces a comprehensive change in how organisations must operate within the European digital setting, moving from isolated product-focused security to a holistic approach that emphasises organisational maturity.

Companies will be required to implement advanced governance through documented policies, rigorous internal processes, comprehensive control mechanisms, and risk management structures that transcend traditional technical boundaries. As the certification framework expands to encompass cloud services, 5G networks, managed security services, and overall cyber posture, technology providers will face heightened regulatory scrutiny and extended time-to-market cycles, even as their clients benefit from verified security standards.

Crucially, the introduction of high-risk supplier mechanisms necessitates a proactive approach to supply chain resilience. This forces entities to assess geopolitical dependencies and monitor interconnected infrastructure. Organizations must, therefore, prepare for the potential replacement of hardware and revise contractual frameworks to mitigate the operational shocks of supplier reclassification.

For small and medium-sized enterprises, this shift creates a dual challenge. Increased reliance on certified vendors may simplify security management while simultaneously driving up procurement costs. Consequently, these firms will require a higher degree of technical due diligence to remain competitive.

On the operational side, the centralisation of reporting through ENISA's unified platform will significantly intensify obligations for "*Security Operations Centres*" ("**SOCs**"). These entities, alongside "*Computer Security Incident Response Teams"* ("**CSIRTs**"), must integrate deeply with EU-level reporting systems. While this improves situational awareness across the Union, it also introduces considerable administrative burdens.

Next steps

The proposal will follow the ordinary legislative procedure, requiring both the European Parliament and the Council to adopt their respective amendments. Afterwards, it will enter a phase of interinstitutional negotiations and technical refinement, aimed at balancing security measures with the practical needs of the market.

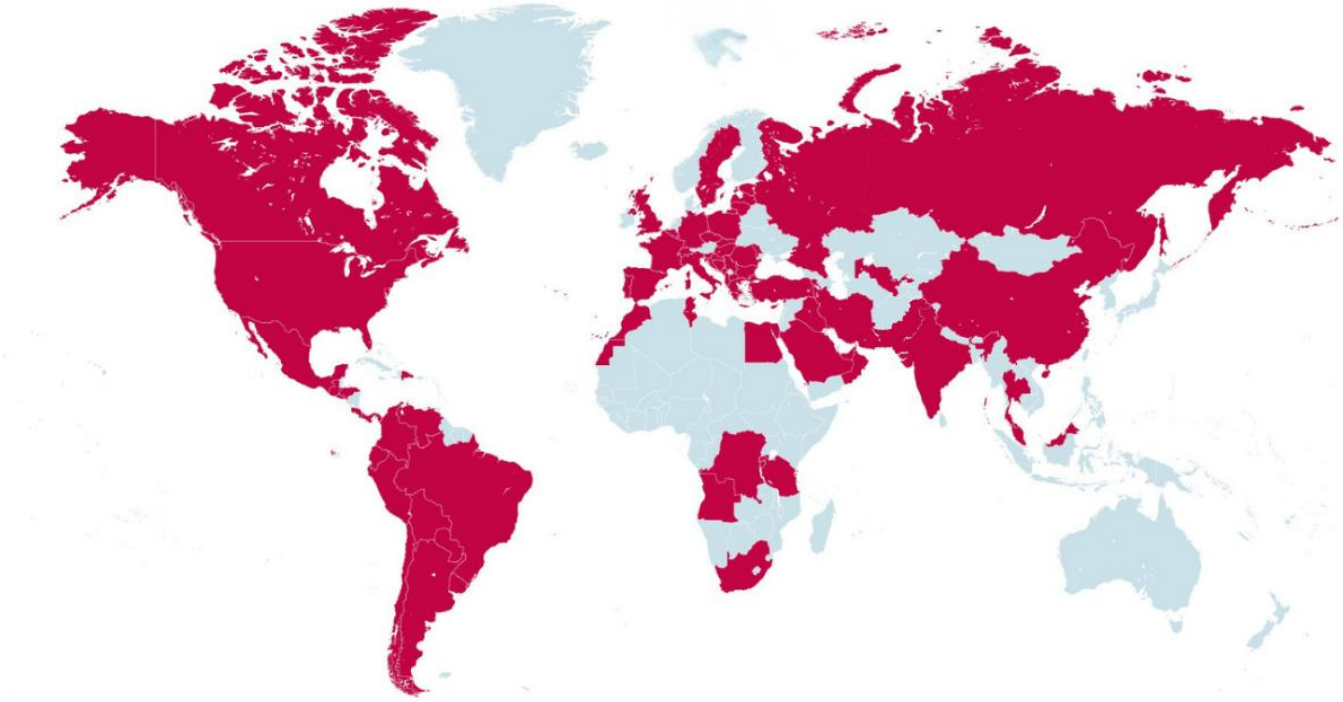
Conclusion

The proposed reform of the "*EU Cybersecurity Act*" signals a transition from fragmented technical standards to a unified, geopolitically aware governance model.

- The consolidation of powers around the European Union Agency for Cybersecurity reduces national divergence and centralises threat reporting and operational coordination at EU level.
- Certification is now a tool for technological resilience rather than just a quality mark. The power to exclude high-risk suppliers in critical sectors forces a fundamental reassessment of third-party dependencies and hardware lifecycles.
- Closer alignment between certification schemes and horizontal product legislation increases the regulatory weight of EU certificates in determining market access and competitive positioning.
- Cybersecurity becomes a board-level responsibility, requiring integrated risk management, structured oversight to ensure alignment with enhanced EU-wide reporting obligations.

GA ALLIANCE

Global legal&tax Advisor



Corso Europa, 12
20122 MILAN, Italy
Tel.: +39 02 30309330

Via Pinciana, 25
00198 ROME, Italy
Tel.: +39 06 45206220

Via Alessandro Maria Calefati, 6
70121 BARI, Italy
Tel.: +39 080 8642350

Strada della Repubblica, 57
43121 PARMA, Italy
Tel.: +39 0521 239489

Galleria dei Borromeo, 3
35137 PADUA, Italy
Tel.: +39 049 8775811

Palazzo Farina
Via Sigismondo, 46
47900 RIMINI, Italy

Via della Zecca, 1
40121 BOLOGNA, Italy
Tel.: +39 051 407 3200

Via Posillipo, 9
80123 NAPLES, Italy
Tel.: +39 081 19623100

Via Locatelli, 3
37122 VERONA, Italy
Tel.: +39 045 8097000

Via Maria Vittoria, 6
10123 TURIN, Italy
Tel.: +39 011 544178

Via San Nicolò, 42
31100 TREVISO, Italy
Tel.: +39 0422 1626262

Via Lazzaretto Vecchio, 5
34123 TRIESTE, Italy
Tel.: +39 040 957 0610

Boulevard Charlemagne 23
1000 BRUXELLES, Belgium
Tel.: +32 2 551 1201

48 Gresham Street
LONDON EC2V 7AY, England
Tel.: +44 (0) 207 183 6423

63 Boulevard Malesherbes
75008 PARIS, France
Tel.: +33 (0)6 68 06 03 57

Via Carlo Frasca, 8
6900 LUGANO, Switzerland
Tel.: +41 (0) 91922 24 80

27 West 20th St. - Suite 1004
10011 NEW YORK, USA
Tel.: +1 9293098424

ALBANIA HOXHA, MEMI & HOXHA | ANGOLA FBL ADVOGADOS | ARGENTINA ALLONCA ABOGADOS | ARMENIA LEGELATA LLC BOLIVIA VIVANCO & VIVANCO | BOSNIA AND HERZEGOVINA DIMITRIJEVIĆ & PARTNERI | BRAZIL DRUMMOND ADVISORS BULGARIA DIMITROV, PETROV & CO. | BURUNDI AFRICASE | CANADA LOTZ & COMPANY | CHILE VIVANCO & VIVANCO | CHINA YINGKE LAW FIRM | COLOMBIA MONCADA ABOGADOS | COSTA RICA VIVANCO & VIVANCO | CROATIA BDV LEGAL | CYPRUS DRAKOPOULOS | CZECH REPUBLIC URBAN & HEJDUK | DEMOCRATIC REPUBLIC OF THE CONGO AFRICASE | DOMINICAN REPUBLIC VEGA IMBERT & ASOCIADOS | ECUADOR VIVANCO & VIVANCO | EGYPT ALC ALIELDEAN WESHAHI & PARTNERS | EL SALVADOR MELARA & ASOCIADOS | ESTONIA KLAUBERG BALTICS | GERMANY SLB LAW GREECE DRAKOPOULOS | GUATEMALA GRAZIOSO BONETTO & ASOCIADOS | HONDURAS GUFA LAW | HONG KONG JUSTIN CHOW & DE BEDIN SOLICITORS LLP | HUNGARY COLLEGIUM BITAI & PARTNERS | INDIA SATINDER KAPUR & ASSOCIATES IRAN SABETI & PARTNERS | IRAQ MUAYAD & ASSOCIATES | LATVIA KLAUBERG BALTICS | LITHUANIA KLAUBERG BALTICS LUXEMBOURG BONN & SCHMITT | MALAYSIA GLT LAW | MALTA CAMILLERI CASSAR ADVOCATES | MEXICO MORENO LAW MOLDOVA BEJAN LAW | MONTENEGRO BOJOVIĆ, DRAŠKOVIĆ, POPOVIĆ & PARTNERS | MOROCCO ELAJOUTI AVOCATS NORTH MACEDONIA APOSTOLSKA LEKSANDROVSKI & PARTNERS | OMAN BAITULHIKMA LAWYERS | PAKISTAN AXIS LAW CHAMBERS | PANAMA CARLES ABOGADOS LAW FIRM | PARAGUAY LEGAL CORPY ADVOGADOS & CONSULTORES PERÙ VIVANCO & VIVANCO | POLAND KOPOCZYNSKI LAW FIRM | PORTUGAL VALADAS CORIEL & ASSOCIADOS | ROMANIA HRISTESCU & PARTNERS | RUSSIA LINNIKOV & PARTNERS | RWANDA AFRICASE | SAUDI ARABIA MAK LAW FIRM, MITHAQ LAW FIRM, ALC ALIELDEAN WESHAHI & PARTNERS | SERBIA BOJOVIĆ, DRAŠKOVIĆ, POPOVIĆ & PARTNERS | SLOVAK REPUBLIC VOJČÍK PARTNERS, S.R.O. | SLOVENIA KIRM PERPAR LAW FIRM | SOUTH AFRICA ADAMS & ADAMS | SPAIN CASTELLANA 170, ABOGADOS | SWEDEN SALC | SWITZERLAND STUDIO LEGALE CUGINI - STELVA | TANZANIA AFRICASE THAILAND ILCT | TUNISIA BERJEBLAWYERS | TURKEY BALAY, ERYIĞIT ERTEN LAWYER PARTNERSHIP | UAE SALT & ASSOCIATES | URUGUAY BERGSTEIN | USA GRANATO OFFICE LAW, MELCHIONNA LAW | UZBEKISTAN ABACUS LAW VENEZUELA TRAVIESO EVANS ARRIA & RENGEL