This translation is a working document. Only the French version is authentic.

OPINION N°2026-06 OF MAY 6TH 2026
ON THE CYBERSECURITY ACT 2

Having regard to Regulation (EU) 2019/881 of the European Parliament and of the Council of April 17th 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)[1]

Having regard to the proposal for a regulation on the European Union Cybersecurity Act published on January 20th 2026[2]

Having regard to Opinion No. 2024-05 of September 4th 2024 of the CSNP on political and economic issues of the European Safety Certification Scheme for Cloud Services (EUCS)[3]

Having regard to the hearings of the Agence nationale de la sécurité des systèmes d'information (ANSSI[4]) and the Direction générale des entreprises (DGE[5]) of the Ministère de l'Economie, des Finances, de la Souveraineté Industrielle, Energétique et Numérique (MEFSIEN[6])

For the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) :
Mr Vincent Strubel, Director-General
Ms Laurence Begou, Deputy Chief of Staff

For the Direction Générale des Entreprises (DGE)
Mr Loïc Duflot, Head of the Digital Economy Division
Mr Renaud Rodenas, Head of Cloud and Data Economy Regulatory Affairs
Ms Edith Guignabaudet, European Affairs Adviser
Ms Shanna Leduc Morin, Cloud and Data Regulatory Framework Officer

Following these consultations and its deliberations, the members of the Commission supérieure du numérique et des postes (CSNP[7]) wish to set out the following recommendations:

Recommendation n°1: Require, during negotiations at the Council of the European Union, the inclusion of explicit articulation clauses ensuring that a certification obtained under the CSA 2 constitutes a presumption of conformity for the equivalent technical requirements of the NIS 2 Directive, DORA and the CRA.

Recommendation n°2: Limit the scope of the cyber posture certification of entities so that it does not replace the audit, supervisory and sanctioning powers of national and sector-specific supervisory authorities.

Recommendation n°3: Restrict the scope of the Single Reporting Platform managed by ENISA in order to prevent risks of overload and confidentiality breaches arising from the centralised transit of critical incident data. Require, for entities operating in the field of national security, a strict derogation ensuring that their incident reports remain under the exclusive competence of ANSSI.

[1] Regulation - 2019/881 - EN - EUR-Lex
[2] Proposal for a Regulation for the EU Cybersecurity Act | Shaping Europe's digital future
[3] Opinion-2024-05-of-the-CSNP-on-the-EUCS-September-4th-2024.pdf
[4] French National Cybersecurity Agency
[5] Directorate-General for Enterprises
[6] French Ministry of Economy, Finance and Industrial, Energy and Digital Sovereignty
[7] High Committee on Digital and Postal Sectors

Recommendation n°4: Request that the European Commission produce a detailed impact assessment evaluating the cumulative financial and administrative burden of the CSA2, NIS 2, DORA and the CRA on European businesses.

Recommendation n°5: Firmly oppose Article 16 of the draft regulation, which provides for the centralisation of unpatched vulnerabilities within a European database managed by ENISA, in order to preserve ANSSI's sovereign control over vulnerabilities affecting critical national infrastructure.

Recommendation n°6: Defend a positioning of ENISA strictly limited to coordination and information sharing, by blocking any transfer of operational incident response capabilities to the detriment of national CSIRTs.

Recommandation n°7: Ensure that the adoption of the CSA 2 preserves France's ability to maintain the SecNumCloud qualification issued by ANSSI, unless a European cybersecurity certification scheme offering an equivalent level of protection, notably in terms of immunity to non-European legislation with extraterritorial reach, were to be adopted.

Recommendation n°8: Amend Articles 19 to 23 to require that the Cybersecurity Skills Academy be built on the mutual recognition of existing national frameworks, such as SecNumedu in France, rather than on the creation of a European mechanism for the direct authorisation of training providers.

Recommendation n°9: Require that the introduction of new fees taken directly from economic actors for the issuance of authorisations and maintenance of certification schemes does not operate to the detriment of budgets allocated to national agencies, and that this mechanism does not increase the financial burden on businesses seeking to raise their security standards and achieve compliance.

Recommendation n°10: Promote at European level a definition of cybersecurity anchored in its technical fundamentals (availability, integrity and confidentiality) affirming that any foreign legislation enabling covert access to data constitutes a technical vulnerability in its own right.

Recommendation n°11: Reject the dichotomy drawn by Recitals 77 and 129 of the draft regulation, which artificially excludes exposure to extraterritorial legislation from the scope of the technical conformity assessment.

Recommendation n°12: Make France's support for the proposal conditional on the reintegration of state-induced legal compromise risks into the assessment frameworks of Title III on certification.

Recommendation n°13: Request a revision of Article 80(1) to clarify how providers subject to laws such as the US FISA can legally fulfil the obligation to "resist any event" compromising confidentiality.

Recommendation n°14: Make France's support for the adoption of any certification scheme conditional on the guarantee that certified providers are not subject to *gag orders*, since such orders structurally prevent them from fulfilling the obligation to report unauthorised access required under Article 80(1)(d).

Recommendation n°15: Draw the Council's attention to the legal risk borne by user entities that, by relying on a misleading European certificate, would find themselves in a situation of non-compliance with their own risk management obligations under NIS 2 and DORA.

Recommendation n°16: Demonstrate the inadequacy of Title IV (administrative police and ban logic) for the cloud services market, and require the creation of positive market-based tools enabling businesses to choose immune solutions without waiting for an exclusion decision by the Commission.

Recommendation n°17: Amend Article 115 on penalties to ensure that fines of up to 7% of total global annual turnover do not fall on user entities alone, but also engage the joint liability of providers when the non-compliance is of their making.

Recommendation n°18: Revise the exemption mechanism of Article 105 in order to drastically reduce the 9-month processing period and to define objective criteria, thereby ensuring legal predictability for economic actors, alongside a provisional operational continuity regime.

Recommendation n°19: Articulate Title IV with Title III by establishing that a service holding a validated immunity certificate is automatically exempt from supply chain restrictions.

Recommendation n°20: Amend Title III to create an extraterritorial legislation immunity label, designed as an optional module applicable across all assurance levels “basic”, “substantia” and “high”.

Recommendation n°21: Build a coalition of Member States in favour of this modular approach, demonstrating that it provides a way out of the diplomatic deadlock over the “High+” level of the EUCS while preserving the openness of the European market.

Recommendation n°22: Defend the principle of voluntary opt-in to this modular label, leaving each business or public administration free to calibrate its legal coverage based on its own risk assessment of data sensitivity.

Recommendation n°23: Ensure that this modular label proactively addresses the needs of essential and important entities under the NIS 2 Directive and financial institutions subject to DORA, which will need to demonstrate the impermeability of their information systems under future obligations imposed by Union law.

I. Background

In April 2019, the adoption of the European Cybersecurity Act (EU) 2019/881 constituted a major step forward by establishing a harmonised cybersecurity certification framework at European level, covering both evaluation methodologies and the different assurance levels for certification.

That Regulation enabled ENISA, the European Union Agency for Cybersecurity, created in 2004, to:

- contribute to the Union's cybersecurity policy;
- strengthen the trustworthiness of products, services and information and communications technologies (ICT) through cybersecurity certification schemes;
- promote and coordinate cooperation with Member States and Union bodies through knowledge sharing, capacity building and awareness raising for national authorities, particularly national CSIRTs;
- collaborate with key stakeholders to strengthen trust in the connected economy, increase the resilience of the Union’s infrastructure and thereby strengthen the digital security of European society and citizens.

In accordance with the Cybersecurity Act, ANSSI is the National Cybersecurity Certification Authority (NCCA) within the framework of the Cybersecurity Act. In that capacity, ANSSI is responsible for overseeing the proper application of the various European certification schemes in France.

In January 2026, the Commission published a proposal to revise the Cybersecurity Act in order to increase cybersecurity capabilities and resilience and preventing fragmentation of the EU digital single market.

The revision also seeks to strengthen the security of the information and communications technology (ICT) supply chains of the European Union.

In the Commission's view, this draft revision ensures that products to which Union citizens have access are cybersecure by design through a simpler certification process.

The draft revision substantially strengthens the powers of the EU Agency for Cybersecurity (ENISA).
The European Commission has opened a public consultation which will close on May 12th 2026.

Through this opinion, the Commission supérieure du numérique et des postes (CSNP) has sought to participate in that consultation by formulating recommendations and drawing the attention of national and European authorities to several key concerns.

II. History of the Cybersecurity Act and of the European Cybersecurity Certification Scheme for Cloud Services (EUCS)

The development of the European Cybersecurity Certification Scheme for Cloud Services (EUCS) originates in the Cybersecurity Act (CSA 1) of 2019. This proposal's mandate was to establish a reference framework ensuring the security and compliance of cloud service offerings on the European market. The trajectory of this text was profoundly altered by the judgment of the Court of Justice of the European Union of July 16th 2020. By invalidating the Privacy Shield, the Court formally exposed the mass surveillance practices enabled by Section 702 of the US Foreign Intelligence Surveillance Act (FISA). While the Data Privacy Framework ratified in July 2023 now governs personal data, a legal vacuum persists regarding the protection of sensitive and strategically important non-personal data held by European organisations.

To address this vulnerability, the first version of the EUCS provided for a maximum certification level designated "High+", which had not posed any difficulty for any European Member State until 2023. Drawing inspiration from the French SecNumCloud qualification, this security level imposed technical criteria, essentially of a legal nature, of immunity to non-European legislation with extraterritorial reach. The objective was to protect European data against legal orders from foreign intelligence agencies, whether US agencies acting under FISA or Chinese agencies acting under the National Intelligence Law of June 27th 2017.

This proposal triggered a direct offensive from US industry and government. On May 25th 2023, the Computer & Communications Industry Association (CCIA) and the Business Software Alliance (BSA) petitioned the Biden administration. These industry groups condemned the "High+" level as a potential threat to US economic interests and national security. The diplomatic pressure materialised in September 2023 when US Secretary of State Antony Blinken sent a note to the European Commission President, Ursula von der Leyen, warning that the inclusion of immunity criteria would negatively affect economic and security relations between the United States and the European Union. Under this pressure, the European Commission requested that ENISA revise its draft. A new version, stripped of the "High+" level and of any immunity requirement, was presented at the beginning of 2024, and the Commission's Legal Service justified this strategic retreat by arguing that a certification scheme derived from CSA 1 could only contain technical criteria, without defining the meaning of that term.

This renunciation gives rise to a glaring legal contradiction with the CSA 1 of 2019. Article 51 of that Regulation requires certification schemes to protect data against unauthorised access, identify known dependencies and guarantee the traceability of consultations. A reference framework validating cloud services subject to secret orders under FISA runs counter to these legal obligations. Access by third-country intelligence services clearly constitutes unauthorised access within the meaning of European law, rendering the current version of the EUCS legally deficient.

It was in reaction to this backdrop that the CSNP adopted its opinion of September 4th 2024. That document alerted public authorities to the extent of the concession entailed by the removal of the "High+" level. The CSNP underlined that data confidentiality requires protection not only against isolated criminal acts but also against lawful interception by foreign powers for economic intelligence purposes. The opinion systematically dismantled the argument that immunity criteria would violate the rules of the World Trade Organisation, since compliance with treaties is assessed at the level of the use of the reference framework in public procurement, not at the level of its technical definition.

Supported by the concerns expressed by the Commission nationale de l'information et des libertés (CNIL[8]) in July 2024, the CSNP formally requested that the French Government require the suspension of the adoption of this weakened EUCS. It called for an economic analysis of the consequences of dependence on the US cloud industry, positioning the reintegration of immunity criteria as a non-negotiable condition for the emergence of an autonomous European technology industry.

It is in this context that the European Commission published, on 20 January 2026, its draft revision of the Cybersecurity Act (CSA2).

Furthermore, this publication comes at a time when the European Commission is also preparing the Cloud and AI Development Act (CADA), expected to be presented before the summer of 2026, which should address, among other matters, the conditions of access to European public procurement in these sectors.

The CSNP considers these two workstreams to be inseparable: it is necessary to anticipate the work on the CADA by establishing, now, the principle that certification schemes adopted under the CSA2 must explicitly integrate protection against extraterritorial legislation to which non-European providers are subject, and that any public procurement falling within the scope of these schemes should require such providers to comply with those requirements.

III. Analysis of the CSA 2: Increased complexity and risk of regulatory incoherence

The proposed revision of the Cybersecurity Act is a text of considerable technical and legal density that sits within an already saturated European legislative ecosystem. To understand what is at stake, one must assess how this new regulation interacts or intersects with a significant number of other major instruments. The European Commission itself acknowledges risks of incoherence, or even direct contradictions, with the NIS 2 Directive, which sets the general framework for risk management for entities classified as essential or important, and the Cyber Resilience Act (CRA), which imposes security rules for all digital products. If the CSA 2 is not aligned with DORA (the Digital Operational Resilience Act), with the CRA or with NIS 2, to mention only these three essential texts, business leaders face an unacceptable legal and criminal uncertainty regarding their own obligations.

This concern is all the more acute given that the CSA 2 is no longer limited to the certification of products, services and processes such as the cloud. The text considerably extends its scope by

[8] National Commission of Information and Freedoms

introducing the certification of managed security services (MSS) and, more fundamentally, the certification of the cyber posture of entities. This major development is intended to enable a business to demonstrate overall compliance with instruments such as NIS 2 or DORA through a certificate. Yet, by shifting certification from the product to the organisation itself, the CSA 2 directly undermines the audit and supervisory powers of sectoral and national supervisors. This shift raises a major difficulty: the cyber posture of an organisation is by its very nature dynamic. It evolves on a daily basis to adapt to new vulnerabilities and constantly changing threats. On the other hand, the issuance of a certificate attests to compliance at a given point in time. This mismatch makes the certification tool unsuitable as a substitute for the continuous and iterative supervision exercised by national control authorities such as ANSSI, whose mission is precisely to assess and guarantee the operational resilience of the most sensitive entities in the face of a constantly evolving technological and geopolitical threat.

To this core framework should be added texts currently under development, such as the forthcoming Cloud and AI Development Act (CADA) and the Digital Networks Act (DNA) for telecommunications infrastructure. For businesses and public administrations alike, this accumulation of regulatory layers, each with its own compliance, reporting and certification requirements, threatens to create major operational uncertainty.

Admittedly, the Commission attempts to respond to this regulatory inflation by tasking ENISA with establishing a Single Reporting Platform. While this initiative moves in the direction of a welcome simplification by aiming to allow businesses to report cyber incidents once for all relevant regulations, it does not address the underlying problem. If coordination between the certification requirements of the CSA 2 and the risk management obligations dictated by these other instruments is not seamless and free of contradictions, organisations risk exhausting themselves in compliance bureaucracy at the expense of their actual technical protection.

Recommendation n°1: Require, during negotiations at the Council of the European Union, the inclusion of explicit articulation clauses ensuring that a certification obtained under the CSA 2 constitutes a presumption of conformity for the equivalent technical requirements of the NIS 2 Directive, DORA and the CRA.

Recommendation n°2: Limit the scope of the cyber posture certification of entities so that it does not replace the audit, supervisory and sanctioning powers of national and sector-specific supervisory authorities.

Recommendation n°3: Restrict the scope of the Single Reporting Platform managed by ENISA in order to prevent risks of overload and confidentiality breaches arising from the centralised transit of critical incident data. Require, for entities operating in the field of national security, a strict derogation ensuring that their incident reports remain under the exclusive competence of ANSSI.

Recommendation n°4: Request that the European Commission produce a detailed impact assessment evaluating the cumulative financial and administrative burden of the CSA2, NIS 2, DORA and the CRA on European businesses.

IV. Preserving the balance of powers between ENISA and national authorities

Title II of the draft regulation provides for a substantial expansion of the mandate and resources of the European Union Agency for Cybersecurity, ENISA. While strengthening European cooperation is an absolute necessity, this ambition must not translate into excessive centralisation that would weaken national security authorities such as ANSSI in France, or national computer security incident response teams (CSIRTs), including CERT-FR. The cybersecurity ecosystem requires, above all, agility and a

thorough understanding of the local economic and industrial fabric. A transfer of operational competences from the national to the European level would risk giving rise to administrative burden and an unacceptable loss of effectiveness. At a time when threats are intensifying at lightning speed, fuelled by the malicious use of generative artificial intelligence and, in the future, by the capabilities of quantum decryption, our collective resilience depends first and foremost on the agility of our frontline response forces.

Furthermore, Article 16 of the draft regulation provides for ENISA to maintain a European vulnerability database and to develop a common Union vulnerability management service capacity. While this initiative aims to strengthen shared threat knowledge, it raises serious concerns regarding its application to the most protected sectors of activity, such as defence or operators of vital importance. From ANSSI's perspective, the centralisation of highly sensitive technical data relating to unpatched vulnerabilities within a single European platform constitutes in itself a major strategic target. Article 16(b) indeed tasks ENISA with developing a "common Union vulnerability management service capacity". Recital 39 justifies this centralisation on the grounds of avoiding duplication of effort, but it paradoxically establishes a single point of failure of the highest strategic importance for national interests. The existence of such a centralised database creates a risk of comprehensive compromise that could expose our national critical infrastructure before remediation measures are even implemented. Sovereign control over vulnerability information affecting the most critical assets must remain exclusively with the national security authority, in order to prevent any premature or inappropriate disclosure that could damage the fundamental interests of the nation. Such centralisation would also risk diluting responsibilities and undermining the effectiveness of the national response in the event of a cyber crisis. Furthermore, and this is an essential point of incoherence, the creation of this single European database runs counter to the very philosophy of decentralisation and proportionality promoted by the NIS 2 Directive.

A similar concern surrounds the new ENISA powers in the area of individual competence certification (Cybersecurity Skills Academy). Articles 19 to 23 of the draft confer on the European agency the power to develop competence attestation schemes and to directly authorise training providers. This centralisation at European level risks bypassing national authorities and existing frameworks, such as SecNumedu in France, which have proven effective in structuring local educational and professional ecosystems. ENISA should build on national frameworks rather than seeking to directly regulate the training and certification market for professionals within each Member State.

In this context, ENISA's role must remain that of a catalyst facilitating coordination and information sharing between Member States, and not that of a substitute authority. The European agency is not designed to dilute the competence of national centres of excellence in order to compensate for the chronic underinvestment or permissive policies of some of our European partners.

Finally, particular vigilance should be paid to the evolution of ENISA's financing model. The draft estimates ENISA's budget at €341 million over the 2028-2034 period, an annual average of €49 million. This sharp budgetary increase would be partly funded through the introduction of new fees levied directly on economic actors for the issuance of authorisations and the maintenance of certification schemes. It is imperative to ensure that this new European levy mechanism does not create a crowding-out effect to the detriment of budgets allocated to national agencies, and above all that it does not increase the financial burden on businesses that are proactively seeking to raise their security standards and achieve compliance.

Recommendation N° 5: Firmly oppose Article 16 of the draft regulation, which provides for the centralisation of unpatched vulnerabilities within a European database managed by ENISA, in order to preserve ANSSI's sovereign control over vulnerabilities affecting national critical infrastructure.

Recommendation n°5: Firmly oppose Article 16 of the draft regulation, which provides for the centralisation of unpatched vulnerabilities within a European database managed by ENISA, in order to preserve ANSSI's sovereign control over vulnerabilities affecting critical national infrastructure.

Recommendation n°6: Defend a positioning of ENISA strictly limited to coordination and information sharing, by blocking any transfer of operational incident response capabilities to the detriment of national CSIRTs.

Recommandation n°7: Ensure that the adoption of the CSA 2 preserves France's ability to maintain the SecNumCloud qualification issued by ANSSI, unless a European cybersecurity certification scheme offering an equivalent level of protection, notably in terms of immunity to non-European legislation with extraterritorial reach, were to be adopted.

Recommendation n°8: Amend Articles 19 to 23 to require that the Cybersecurity Skills Academy be built on the mutual recognition of existing national frameworks, such as SecNumedu in France, rather than on the creation of a European mechanism for the direct authorisation of training providers.

Recommendation n°9: Require that the introduction of new fees taken directly from economic actors for the issuance of authorisations and maintenance of certification schemes does not operate to the detriment of budgets allocated to national agencies, and that this mechanism does not increase the financial burden on businesses seeking to raise their security standards and achieve compliance.

V. The imperative of coherence in defining cybersecurity risks

To grasp what is at stake, it is necessary to return to the fundamentals of the doctrine in this area as digital security rests on three inseparable pillars, often referred to as the CIA triad : confidentiality, integrity and availability. Confidentiality ensures that only authorised persons have access to data. Integrity ensures that information is neither modified nor altered in an illegitimate manner. Availability, finally, ensures that systems and data are accessible at the precise moment when the user needs them. In the context of a risk assessment legitimately conducted by a business or public administration, any event capable of compromising one of these three pillars is treated as a security threat regardless of its origin.

Yet, the Commission's draft text attempts to introduce a confusing distinction between risks classified as "technical" and those classified as "non-technical". Under this logic, a software vulnerability exploited by a hacker would be a technical risk, while a foreign legal order requiring a provider to covertly but lawfully hand over data, notably in the context of economic intelligence activity, would be considered a non-technical risk. From the perspective of a user organisation that must protect its industrial secrets or sensitive and strategically important data, this separation is pure legal fiction, as the operational consequence is strictly identical: in both cases, confidentiality is breached and the damage to the entity is total. The same applies to availability, if a service is unilaterally interrupted by a provider in order to comply with a diplomatic retaliation measure of its home state: for the European user, this constitutes a technical interruption of business continuity. European certification therefore cannot be emptied of its substance by ignoring these vectors of insecurity on the pretext that they are of legal or state origin.

This artificial dichotomy is embedded in the very architecture of the text. Recital 77 states that the certification framework, Title III, must focus on technical risks, while Recital 129 relegates exposure to the jurisdiction of a third country to the category of "non-technical" risk. This separation deprives users of the ability to technically attest to the actual confidentiality of their data in the face of extraterritorial

legislation. On the contrary, a provider's exposure to legislation with extraterritorial reach must be analysed as a structural vulnerability, in the same way as a software design flaw, that degrades the overall security performance of the service. For a European business, a foreign law with extraterritorial reach, such as Section 702 of the US FISA or Article 7 of the Chinese National Intelligence Law of June 27th 2017, clearly creates a vulnerability in the technical dependency chain of the digital service subject to it, making it a substantive operational security deficiency and not merely a geopolitical issue that could be left, without legal guarantees, to the sole appreciation of Member States or the European Commission.

Recommendation n°10: Promote at European level a definition of cybersecurity anchored in its technical fundamentals (availability, integrity and confidentiality) affirming that any foreign legislation enabling covert access to data constitutes a technical vulnerability in its own right.

Recommendation n°11: Reject the dichotomy drawn by Recitals 77 and 129 of the draft regulation, which artificially excludes exposure to extraterritorial legislation from the scope of the technical conformity assessment.

Recommendation n°12: Make France's support for the proposal conditional on the reintegration of state-induced legal compromise risks into the assessment frameworks of Title III on certification.

VI. The paradox of impossible compliance under Article 80(1)

Article 80(1) of the draft regulation sets out the security objectives that every future European certification scheme will be required to pursue. As such, this Article constitutes the trust foundation of the entire framework. Paragraph (v) of that Article requires all certified services to "resist any event" liable to compromise the confidentiality, authenticity, integrity or availability of data and associated processing operations. The scope of the expression "any event" is fundamental here: in the absence of an explicit restriction to incidents of technological origin alone, it includes de facto administrative or judicial orders.

This wording creates an insurmountable legal impasse for providers subject to extraterritorial legislation such as Section 702 of the US FISA or Article 7 of the Chinese National Intelligence Law of June 27th 2017. The impasse is all the more manifest in that the first point of Recital 137 explicitly acknowledges that certain third countries require entities under their jurisdiction to report software vulnerabilities to their own authorities before any public disclosure. This foreign provision makes it legally impossible for a provider to fulfil the incident transparency obligation set out in Article 80(1)(d). It should be recalled that Section 702 of FISA allows US intelligence agencies to require access to data belonging to non-US persons from cloud providers subject to US law, without a judicial warrant. These actors are legally required to cooperate with their intelligence authorities and cannot, without violating their own national law, "resist" such a data handover order or a mechanism for the unilateral interruption of services. A very concrete example of this was provided with the sanctions imposed in 2025 on judges of the International Criminal Court, including our fellow citizen Judge Nicolas Guillou.

This contradiction is aggravated by the artificial distinction the text attempts to draw between so-called "technical" and "non-technical" risks. By arbitrarily classifying exposure to a third-country jurisdiction in the latter category, the Commission ignores the operational reality of organisations for which covert access to their data constitutes a technical breach of confidentiality as serious as a cybercriminal intrusion. By ignoring this conflict of laws, the Regulation deliberately organises an impossibility of compliance: either the provider obtains a certificate despite a documented legal vulnerability, or the certificate is issued on the basis of a capacity for resistance that the provider is structurally unable to offer.

Such a framework places businesses leaders and public administrations in a situation of major legal uncertainty, as it would lead them to believe in a protection that does not exist, while depriving them of the information necessary for their own regulatory compliance, notably under the NIS 2 Directive or DORA. Moreover, this opacity directly contradicts Article 80(1)(d), which requires reporting of unauthorised access: the application of foreign non-disclosure orders (gag orders) would make it legally impossible for the provider to fulfil this transparency obligation towards its European clients and supervisory authorities.

Recommendation n°13: Request a revision of Article 80(1) to clarify how providers subject to laws such as the US FISA can legally fulfil the obligation to "resist any event" compromising confidentiality.

Recommendation n°14: Make France's support for the adoption of any certification scheme conditional on the guarantee that certified providers are not subject to *gag orders*, since such orders structurally prevent them from fulfilling the obligation to report unauthorised access required under Article 80(1)(d).

Recommendation n°15: Draw the Council's attention to the legal risk borne by user entities that, by relying on a misleading European certificate, would find themselves in a situation of non-compliance with their own risk management obligations under NIS 2 and DORA.

VII. An ICT supply chain security mechanism (Title IV) in need of improvement

The new Title IV of the draft regulation introduces a framework designed to secure ICT supply chains within the European Union. This mechanism rests on an "administrative police" logic activated at the sole discretion of the European Commission: after conducting risk assessments, the Commission could designate identified suppliers as "high-risk suppliers" and consequently prohibit or restrict the use of their products and services by European essential entities. While such a mechanism may appear legitimately designed and potentially effective for protecting tangible hardware infrastructure, such as telecommunications network equipment, it proves entirely inoperative when applied to the cloud services domain.

The major contradiction of this mechanism lies in its binary and political nature. As long as a provider has not been officially banned by the Commission, users cannot invoke any legal guarantee of immunity. Yet a "high-risk supplier" designation targeting major US cloud providers would make no economic or diplomatic sense. No one in Europe seeks the exclusion of these actors, whose technological contribution remains essential to the competitiveness and digital transformation of our economy. Furthermore, in the current state of relations with our strategic partners, such a decision would be perceived as a catastrophic diplomatic retaliation measure that no one calls for.

As currently drafted, this mechanism therefore places businesses and public administrations in an impasse. It perpetuates the status quo of an involuntary exposure to extraterritorial legislation without giving the market the slightest legally binding lever to guard against it. For cloud services, the need of the final beneficiaries of certification does not lie in the political banning of major providers, but in the freedom to be able to require and choose, for their most sensitive and strategically important data, environments offering strict legal guarantees of confidentiality and availability. Failing to provide this predictability and these market-based tools, Title IV misses its objective of reinforcing the security of data processing in favour of a purely discretionary management of geopolitical risks. This uncertainty is aggravated by the exemption regime provided for in Article 105: an entity controlled by a third country may request exemption from the prohibitions. However, with a 9-month response period left to the Commission and discretionary assessment criteria, this mechanism amplifies economic

uncertainty where an optional and immediately available immunity label under Title III would provide the essential market predictability.

The legal uncertainty into which this mechanism plunges businesses is all the more unacceptable in that it is accompanied by financial penalties of unprecedented severity. Article 115 of the draft regulation provides for fines of up to 7% of total global annual turnover for businesses infringing the prohibitions relating to high-risk designated suppliers. Imposing such criminal and financial risk exclusively on user organisations, while denying them the legal means and clear certification labels to require the immunity of their providers in advance, constitutes at the very least a serious source of concern.

To break this impasse, a structural link between Title III, dedicated to certification, and Title IV, dedicated to supply chain security, is indispensable. The exemption regime under Article 105 requires an entity to demonstrate the effectiveness of its mitigation measures against foreign interference. Yet this is precisely the purpose of a rigorous technical certification scheme. Accordingly, the technical and audited validation obtained through an immunity label under Title III constitutes an objective and sufficient proof to remove the inherent uncertainties of Title IV's administrative police logic. Establishing that a service certified with this level of guarantee is automatically exempt from supply chain restrictions would create a major simplification bridge. This fast-track mechanism would restore immediate legal predictability for economic actors: trust would be guaranteed a priori through technical and market-based compliance, rather than being suspended on a political and administrative decision a posteriori.

Recommendation n°16: Demonstrate the inadequacy of Title IV (administrative police and ban logic) for the cloud services market, and require the creation of positive market-based tools enabling businesses to choose immune solutions without waiting for an exclusion decision by the Commission.

Recommendation n°17: Amend Article 115 on penalties to ensure that fines of up to 7% of total global annual turnover do not fall on user entities alone, but also engage the joint liability of providers when the non-compliance is of their making.

Recommendation n°18: Revise the exemption mechanism of Article 105 in order to drastically reduce the 9-month processing period and to define objective criteria, thereby ensuring legal predictability for economic actors, alongside a provisional operational continuity regime.

Recommendation n°19: Articulate Title IV with Title III by establishing that a service holding a validated immunity certificate is automatically exempt from supply chain restrictions.

VIII. The modularity of certification schemes in the service of trust and the market

To understand the scope of the proposed revision of Title III of the Cybersecurity Act, it is necessary to understand the architecture of European certification schemes. The current framework provides that each digital product or service can be certified according to three progressively demanding assurance levels: "basic", "substantial" and "high". The "basic" assurance level focuses on minimising elementary cyber risks, primarily through a review of the technical documentation. The "substantial" assurance level aims to counter attackers with limited capabilities through in-depth checks of security functions. Finally, the "high" assurance level requires resistance to sophisticated cyberattacks carried out by actors with significant resources, validated through rigorous penetration tests.

Since 2021, the European safety certification scheme for cloud services (EUCS) has been deadlocked in a situation that stalls the digital transformation of the Union. The CSNP had published, in September

2024, an opinion to present and document this unacceptable situation in view of the growing cybersecurity challenges in the cloud. This deadlock stems from a binary and unjustified opposition between an approach limiting the scheme to technological criteria and a proposal integrating immunity requirements from non-European legislation with extraterritorial reach at the "high" level only. This polarisation hardened into a sterile antagonism at the end of 2023, following diplomatic pressures aimed at removing all legal trust guarantees from the future European framework.

Faced with this paralysis, the CSNP considers that the way out of these debates lies in a modular approach consisting of strictly decoupling the technological assurance levels from the immunity criteria with respect to non-European legislation with extraterritorial reach. Rather than crystallising the debate around a specific level, the aim should be to create an optional and cross-cutting immunity label that can be associated with each of the three technological levels, basic, substantial or high. This modularity is the only approach capable of restoring market choice and responding to the real diversity of needs of businesses and public administrations.

Although Article 71(3) presents the certification as voluntary, it provides for derogations where Union law so requires. For sectors regulated by DORA or NIS 2, for example, certification will de facto become the sole means of demonstrating rigorous risk management. Without an immunity label, these entities will be legally compelled to certify against a framework that deliberately ignores the risk of foreign interference, at a time when that risk, in the international context in which the European economy operates, has never been greater.

An organisation could thus, according to its own risk analysis, choose a technically sufficient "basic" level service, but supplement it with the immunity label to host sensitive personal data in a manner consistent with the GDPR. Alternatively, an entity processing strategically important industrial data could opt for a "substantial" technical level supplemented by this same label to guard against covert access under Section 702 of the US FISA or the Chinese National Intelligence Law of June 27th 2017. By directly embedding this optional label mechanism in the Regulation, Europe would free itself from debates over a "High+" level, equipping itself instead with a flexible and robust market tool, the only one capable of guaranteeing the strategic autonomy and resilience of our organisations without excluding major technological players.

Recommendation n°20: Amend Title III to create an extraterritorial legislation immunity label, designed as an optional module applicable across all assurance levels "basic", "substantia" and "high".

Recommendation n°21: Build a coalition of Member States in favour of this modular approach, demonstrating that it provides a way out of the diplomatic deadlock over the "High+" level of the EUCS while preserving the openness of the European market.

Recommendation n°22: Defend the principle of voluntary opt-in to this modular label, leaving each business or public administration free to calibrate its legal coverage based on its own risk assessment of data sensitivity.

Recommendation n°23: Ensure that this modular label proactively addresses the needs of essential and important entities under the NIS 2 Directive and financial institutions subject to DORA, which will need to demonstrate the impermeability of their information systems under future obligations imposed by Union law.