EUROSMART
The Voice of the Digital Security Industry

Digital Package and Omnibus – Call for evidence
Eurosmart's Position

While Eurosmart welcomes the Commission's work on the Digital Omnibus, we note with concern that the current Call for Evidence appears to narrow the initial ambition of this initiative. The Omnibus was originally conceived as a bold and strategic exercise to streamline Europe's increasingly complex digital regulatory landscape and to remove inconsistencies between key legislative acts. However, its current scope seems limited to administrative simplification, without sufficiently addressing the substantive overlaps already identified by policymakers and stakeholders.[1]

Eurosmart therefore calls for the Digital Omnibus to fully assume its political and strategic role: ensuring coherence across Europe's digital regulatory landscape, enhancing legal certainty, and enabling innovation grounded in trust, security, and fundamental rights. Beyond necessary administrative simplifications, **Eurosmart believes the true objective of the Omnibus should be to strengthen European competitiveness and reinforce confidence in secure digital technologies.**

Eurosmart has identified several areas where the Digital Omnibus can deliver real impact by harmonsing requirements from different EU legislative instruments, and more generally ensuring consistency across Europe's digital regulatory landscape while enabling a necessary risk-based approach.

[1] The LIBE Committee, for instance, has underlined in its recent exchange of views on 22 September 2025 on the Digital Simplification Package and the Digital Policy Area Fitness Check the urgent need to safeguard fundamental rights and resolve conflicting or redundant provisions across digital acts. Yet, these critical issues remain insufficiently reflected in the Commission's current approach.

Table of Contents

1. Excessive constraints on QSCD certification imposed by eIDAS[2]

The latest amendment to eIDAS regulation substantially strengthened the management of QSCD certificates. As per the article 30.3a which was added, as soon as a vulnerability affecting the security certificate of a QSCD arises, the product certificate is automatically revoked. Practically, it implies that such product becomes unusable, as any subsequently produced electronic signature is not qualified anymore (legally equivalent to handwritten signature). Even if the risk could be mitigated, this has very substantial impacts on suppliers of QSCD, their issuers and users.

While the intention to maintain a high level of trust is understandable, this rigid mechanism can have systemic consequences. It disrupts both public and private sector operations, particularly where QSCDs are used in national ID and trust service infrastructures. In such cases, a single vulnerability that could be mitigated could suddenly invalidate secure identification documents or digital identity tokens - still physically valid, yet technically unusable. This situation directly affects EU citizens' ability to authenticate and sign, and undermines the sovereign continuity of national identity systems, a cornerstone of the European digital identity framework.

eIDAS regulation lacks clear provisions for the management of risks on QSCD, so that when a vulnerability arises, the QSCD certificate could be maintained and it could still be used to produce qualified signature, but under specific conditions allowing to mitigate the risks stemming from that vulnerability. Further details on risk management can be found in a previous Eurosmart's position paper[3].

> **Therefore, Eurosmart recommends updating eIDAS regulation (and more precisely article 30) so that (1) where vulnerabilities are identified, the QSCD certificate is not necessarily cancelled, and (2) where vulnerabilities are identified, the QSCD certificate could be maintained and the QSCD could still be used provided relevant and suitable mitigation measures are put in place.**

2. Interplay between NISD2[4] and the CRA[5]

NISD2 and the CRA are closely intertwined which will create substantial complexity and burden for private sector. The following bottlenecks and excessive burden have been identified which should be removed through an adaptation of NISD2 and/or the CRA:

2.1 Streamlining Compliance for Remote Data Processing Solutions Under the CRA and NISD2

As per the CRA, remote data processing solution (RDPS) shall be considered as being part of a product with digital elements (see article 3.1), which implies that it is also covered by conformity

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183
[3] https://www.eurosmart.com/how-can-we-manage-the-inevitable-security-erosion-of-chip-based-documents-eurosmart-proposes-a-new-approach/
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

assessment. However, it is very likely that some types of remote data processing solutions are also covered by NISD2. This is the case for the installation, management, operation or maintenance of ICT products, whose providers are qualified as "managed service provider[s]" and subject to NISD2 obligations (see article 6(39)). Therefore, it entails that such types of remote data processing solutions are subject to both the CRA and NISD2. As it creates substantial duplication of work, it will result in increased costs, complexity and time to market. Yet, remote data processing solutions covered by NISD2 (e.g. those provided by a managed service providers) are already subject to stringent, risk-based cybersecurity obligations and supervision by competent authorities as per NISD2, and these obligations cover the same security objectives as the CRA's essential requirements. To avoid unnecessary duplication, Eurosmart calls on policymakers to recognise compliance efforts already ensured under NISD2 when assessing conformity of remote data processing solutions with CRA essential requirements.

> **Therefore, Eurosmart recommends that for remote data processing solutions falling under NISD2, conformance to NISD2 serves as evidence of conformance to CRA, limiting or avoiding additional CRA conformance exercises.**

2.2 Avoiding Double Assessment for Products Covered by Both the CRA and NISD2

Some software products with digital elements are exclusively dedicated to being (1) procured by professional users and (2) used as part of a system providing a service covered by NISD2 (critical or important services). In that case, such software products with digital elements are subject to mandatory conformity assessment at their placing on the market (as required by the CRA) and subsequently – once installed, configured and integrated within the system - subject to a security audit before being operated as part of the service covered by NISD2. This double assessment regime increases costs, complexity and time to market for the provision of the products with digital elements.

> **Therefore, Eurosmart suggests that for software products with digital elements exclusively dedicated to being (1) procured by professional users and (2) used as part of a system providing a service covered by NISD2, the conformity assessment as required for the CRA (1) is not carried out prior to the placing on the market but once the software product with digital elements is installed, configured and integrated within the system and ready to be operated, and (2) explicitly relies and leverages NISD2 compliance which already demonstrates fulfilment of CRA requirements.**

3. Interplay between the CRA[6] and the CSA[7]

As per the CRA, a manufacturer can demonstrate conformity of a product with digital elements with the essential cybersecurity requirements using a EU cybersecurity certificate (article 32). However, the CRA requires the Conformity Assessment Bodies under the CSA which are involved in the issuance of that EU cybersecurity certificate to also be accredited under the CRA as Notified Bodies. This constraint makes more complicated to reuse an EU cybersecurity certificate to demonstrate conformity of a product with digital elements with the CRA, as it implies supplemental actions and costs for certification authorities and testing laboratories established

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847
[7] https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

under the CSA. In addition, the lack of clear viability for these supplemental expenses may divert them from completing these supplemental tasks.

> **Therefore, Eurosmart recommends recognizing Conformity Assessment Bodies accredited under ISO/IEC 17025 or ISO/IEC 17065, as required by the Cybersecurity Act (CSA), to facilitate or enable their designation as Notified Bodies under the CRA. This is particularly important to ensure that EU cybersecurity certificates issued under the CSA can be used to demonstrate conformity with the CRA's essential cybersecurity requirements.**

4. Harmonization of conformity assessment practices in the CRA, CSA, NISD2, AI Act[8] and eIDAS

The CRA, CSA, AI Act and eIDAS provide for conformity assessment of products and services. In order to ease recognition and reuse of these conformity assessments across these legal frameworks, the trust and the governance of all these conformity assessment schemes should be harmonized. In that regard, they should rely on international standards for conformity assessment (ISO/IEC 17025) and certification (ISO/IEC 17065) which are widely established and used worldwide.

As conformity assessments under each of these texts are getting more and more intertwined, harmonization of conformity assessment is absolutely required. Examples of such entanglements are (non-limitative):

- Remote data processing which may be covered by the CRA and NISD2;
- Security products which may be covered both by the CRA and CSA;
- Smart contracts covered by the CRA (as they are product with digital elements), and generated by trust services covered by eIDAS (electronic ledger);
- Trust services providers which are covered both by NISD2 and eIDAS;
- Digital identity products assessed under eIDAS and the CRA and whose operation is covered by eIDAS and may be covered by NISD2;
- Security products used for the provision of trust services which are covered by the CRA, and whose operation are covered by eIDAS and NISD2;
- Security products used by entities covered by NISD2 which may be subject to mandatory security certification as per the CSA;

> **Therefore, Eurosmart recommends amending the CRA, CSA, AI Act and eIDAS to require:**
>
> - **Notified bodies carrying out conformity assessments and conformity assessment bodies (under the CSA) to comply with ISO/IEC 17025;**
> - **Notified bodies carrying out certification activities and NCCA (under the CSA) to comply with ISO/IEC 17065;**

[8] https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

5. Harmonisation of vulnerability management.

Currently, each framework (CRA, CSA, eIDAS, GDPR[9]) addresses vulnerabilities in isolation, with different definitions, notification procedures, and consequences for certification or product compliance to essential requirements. This fragmentation creates uncertainty for manufacturers, service providers, and users: particularly when a vulnerability in a certified product under one regulation may trigger disproportionate consequences under another (for example, automatic certificate revocation under eIDAS or loss of conformity under the CRA).

> **Eurosmart proposes that the Digital Omnibus ensures a coherent and risk-based approach by harmonizing vulnerability management across the EU's digital regulatory landscape.**

6. Provide clear legal framework for Common Specifications and technical specifications used to support implementation of legal acts

Several legal texts have introduced the possibility for the European Commission to draft and adopt through implementing acts so called Common Specifications providing presumption of conformity to essential requirements (e.g. CRA, IA Act). These Common Specifications are therefore a new possibility for manufacturer – alongside harmonized standards – to benefit from a presumption of conformity with essential requirements. However, while harmonized standards are ruled by regulation 2012/1025, which provide clear governance for their drafting and adoption, including formal objections from Member States to harmonized standards, such legal framework does not exist for Common Specifications.

> **Therefore, Eurosmart recommends setting up a clear legal framework for Common Specifications, similar to what is provided for in regulation 2012/1025 for harmonized standards, and covering in particular (not limitative):**
>
> - **transparence and involvement of stakeholders and Member States, and clear rules in the drafting and adoption of Common Specifications;**
> - **relation of Common Specifications to harmonized standards including precedence of harmonized standards over Common Specifications once a harmonized standards is adopted over the same scope;**
> - **the role of Member States;**
> - **the mechanisms for formal objections of Member States to Common Specifications as defined for harmonized standards in article 11 of Regulation EC 2012/1025;**

In addition, in other contexts, the European Commission is also tasked with the preparation of technical specifications to support the implementation of a legal text (e.g. eIDAS).

[9] https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Here again, Eurosmart recommends a clear legal framework is needed to clarify:

- the preparation and adoption of these technical specifications;
- their relations to harmonized standards;
- the role of Member States;

7. Enhance the CSA to provide mechanisms for risk management over certified products

The CSA provides a framework for security certification of products, services and processes. Yet, as the security erodes over time, it is ineluctable that a product which was certified at one moment in time loses its security certificate, even when secure operation remains possible and the risk is clearly mitigated.

This may be very problematic in many sectorial legislations (e.g. eIDAS) that require products to hold valid EU cybersecurity certificate issued under the CSA. As it entails that the product can't be used anymore and must be replaced. In some cases, it may not be possible in a reasonable timeframe, or even doable.

However, even when a product loses its EU CSA security certificate, it may still be possible to use it with a high level of security provided relevant mitigation measures are put in place. Indeed, these mitigation measures should be carefully defined based on the risk assessment to ensure they properly address the risks applicable to the specific usage of the product considering its environment of use.

In that regard, alongside "valid" and "revoked", the new state "conditional" should be introduced for the EU CSA security certificate. This state should only be applicable to to products already manufactured and not to those newly produced or placed in the market. In addition, this state should only be granted to products in which a vulnerability has been detected causing its EU CSA cybersecurity certificate not to be "valid" anymore, but for which mitigation measures could be put in place allowing to maintain the overall security of the product for its usage in its environment of use. This state "conditional" should be maintained as long as the overall security of the product can be maintained for its usage in its environment of use through mitigation measures.

In addition, the risk assessment and the mitigation measures should be defined in a multilateral forum gathering the (1) impacted national cybersecurity authorities, (2) the impacted vendor(s) and (3) the issuer of the products on the field" in order to ensure transparency, trust and effectiveness. In that regard, the EU ISAC could be the right forum to organize such cooperation.

Therefore, Eurosmart recommends amending the CSA to

- introduce a new state "conditional" for the EU CSA security certificate;
- restrict this state only to product used on the field and not to product newly produced or placed in the market;
- set in state "conditional" the EU CSA security certificate of product in which a vulnerability has been detected causing its EU CSA cybersecurity certificate not to be "valid" anymore, but for which mitigation measures could be put in place allowing to maintain the overall security of the product for its usage in its environment of use;

- **maintain in state "conditional" a EU CSA security certificate as long as as long as the overall security of the product can be maintained for its usage in its environment of use through mitigation measures;**
- **set up the necessary methodology and governance to define and carry out the risk assessment and the mitigation measures. In that regards, the EU ISAC could be the right forum to organize such cooperation;**

8. Clarification on the implementation of NISD2

NISD2 defines various types of entities which may be classified as essential or important. However, these various types of essential or important entities overlap meaning that an entity could fall within different categories e.g. a provider of qualified certificates could be classified as trust service provider (as part of the digital infrastructure sector) or as a Managed service provider (as part of the ICT service management sector) or Public administration sector if used by public administration. Ultimately, the choice of the type in which an entity falls is up to the applicable jurisdiction which will be in charge of the supervision of that entity.

As per NISD2, the applicable jurisdiction in charge of the supervision of an entity differs depending on its sector and its type, i.e. the applicable jurisdiction may be:

- the Member State(s) where it is established;
- the Member State where they have their main establishment;
- The Member State in which they provide their services;
- The Member State(s) that established them;

As per NISD2 it is possible that the same entity is classified into different types by different jurisdictions. In particular, there is a risk that (1) the Member State where an entity is established or has its main establishment classifies it in such a way that it supervises that entity, and (2) the Member State where that entity provides its services classifies it in such a way that it also supervises that entity. As such, this double supervision would be very detrimental as it would imply increase complexity, costs, conformity activities and time to market for entities.

> **Therefore, Eurosmart recommends preventing the application of multiple criteria and requirements to the same system across Member States and establishing safeguards under NISD2 to ensure that entities are supervised under a single jurisdiction.**

9. Making the AI Act Work

Eurosmart supports the European Commission's efforts to simplify the implementation of the AI Act. With full application less than a year away, industry urgently needs legal clarity and consistent enforcement across the EU, especially for high-risk AI systems. The Digital Omnibus should ensure coherent application of the AI Act, legal predictability, and smooth interaction with other EU legislation.

To achieve these goals, the Commission should consider:

1. The impact of delayed harmonized standards on timely implementation;
2. Criteria for identifying entities eligible for alternative measures;

3. Consistent enforcement across Member States;
4. The EU's ability to benchmark and evaluate AI solutions;
5. The interplay between the AI Act and the GDPR.

9.1 Impact of delayed harmonized standards

The late development of harmonized standards poses a major challenge to timely compliance. It is increasingly unlikely that all relevant standards will be adopted in time for developers of high-risk AI systems to achieve full compliance by August 2026. Companies making genuine efforts to comply risk being unfairly penalized due to factors beyond their control.

> **The Digital Omnibus should therefore allow for a reassessment of the AI Act's initial implementation timeline**. Compliance deadlines should be linked to the official adoption of harmonized standards. **A joint evaluation by the European Commission and the standardization bodies should determine realistic timelines for the adoption of harmonized standards. Based on this analysis, standardization requests should be reviewed or updated accordingly.**

Then, a thorough assessment by the European Commission, conducted with the support of industry, should evaluate the time required for companies to adapt and achieve full compliance with the adopted standards.

9.2 Criteria for alternative measures

Discussions around **special measures for SMEs and small mid-caps often assume a correlation between company size and potential risk**. In high-risk domains such as biometrics, however, the risk to Fundamental rights and personal data is not increasing according to company size or revenue. Larger companies often have established stict compliance and security frameworks.

> **Eurosmart recommends that the Digital Omnibus establish objective, risk-based criteria for any alternative measures, applicable to all deployers of high-risk AI systems. Compliance flexibility should not introduce new risks or undermine the overall security and trustworthiness of AI systems in Europe.**

9.3 Consistent implementation across Member States

The current fragmentation in Member States' designation of national competent authorities demonstrates the risk of inconsistent application. Divergent national approaches would create legal uncertainty and uneven market conditions for European industry.

> **The Digital Omnibus should require Member States to regularly consult with industry and other stakeholders during the implementation process to ensure a coherent and predictable regulatory environment across the EU.** This consultation could build on existing structures established under the AI Act, in particular the AI Board, which brings together representatives from all Member States and is responsible for ensuring the consistent application of the Act throughout the Union.

> **To make this consultation process effective, the AI Act should be amended to formally extend the mandate of the AI Board to include regular coordination and dialogue with industry and other stakeholders on implementation matters.** This extended mandate should also foresee structured cooperation with the Advisory Forum, which gathers representatives from industry, civil society, and academia.

9.4 EU capability to evaluate and benchmark AI systems

The EU must develop its own capacity to assess and benchmark AI systems, based on European values, standards, and security requirements. This is particularly relevant for strategic sectors covered by ProtectEU[10].

> **The Digital Omnibus should launch a process to define the technical and institutional capabilities required to ensure consistent evaluation and oversight of AI systems deployed in Europe. To this end, An amendment to the AI Act should task the Joint Research Centre (JRC) with defining and deployed the technical and institutional capabilities required to ensure consistent evaluation and oversight of AI systems deployed in Europe.**

9.5 Interplay with GDPR

Eurosmart welcomes ongoing efforts by the European Data Protection Board (EDPB) and the Commission to clarify the relationship between the AI Act and the GDPR.

> **However, amendment to GDPR is needed to align with AI Act, particularly regarding biometric systems - such as the distinction between biometric identification and verification as put forward by the AI Act.**

The Digital Omnibus should help clarify overlaps in enforcement and ensure that the AI Act operates in harmony with other EU legislation. Legal clarity in this area is essential to support innovation, competitiveness, and the protection of fundamental rights.

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com