EUROSMART
The Voice of the Digital Security Industry

Eurosmart's answers to Digital Omnibus on AI public consultation

March 2026

Eurosmart, the voice of the European digital security industry, welcomes the European Commission's initiative to introduce a Digital Omnibus on Artificial Intelligence, which proposes targeted amendments to the Artificial Intelligence Act.

As a European association representing companies active in digital security technologies and trusted solutions, Eurosmart closely follows the development and implementation of the European Union's regulatory framework for artificial intelligence. The association supports initiatives that contribute to the effective and predictable implementation of the AI regulatory framework while ensuring a high level of security and trust in digital technologies.

1. Postponement of the entry into application of high-risk AI requirements

Eurosmart supports the overall intention to postpone the entry into application of requirements for high-risk AI systems in order to provide time for standardisation bodies to complete their work.

The revised timeline should provide a high level of legal certainty in order for the industry to prepare accordingly and ensure full compliance on the date of application.

2. Governance for changes to high-risk AI systems and prohibited practices

Any changes to the list of high-risk AI systems in Annex III and to the list of prohibited practices in Article 5 should follow the process laid out in the AI Act.

This process should ensure the full involvement of the AI Office and appropriate consultation of the AI Board and the Advisory Forum.

3. EU-Level AI regulatory sandbox

Eurosmart considers that, in line with the need to provide the Commission with appropriate resources to support research, testing and development activities at EU level, the AI Office should be able to create an EU regulatory sandbox.

4. Processing of special categories of personal data for bias detection and mitigation (Article 4a)

Eurosmart welcomes the introduction of Article 4a concerning the processing of special categories of personal data for bias detection and mitigation.

Articles 4a(1)(c) and (d) define security measures that should apply to such special categories of data. **However, these measures may be insufficient as they do not address the risks of these data being exported, stored or processed outside the EU or the EEA and thus escaping EU or Member State control.** This could create risks such as uncontrolled copying or processing for uncontrolled purposes.

To address this risk, it should be clarified that entities accessing special categories of personal data should:

- not be subject to non-EU or non-EEA laws, whether natural or legal persons;
- for natural persons, be EU or EEA citizens;
- for legal persons, demonstrate that they are not subject to non-EU or non-EEA laws;
- only use components, including software, hardware and cloud services, that are not subject to non-EU or non-EEA laws.

Eurosmart therefore suggests modifying:

- Article 4a(1)(c) to include that special categories of personal data shall only be stored, processed and handled by EU or EEA natural persons and by EU or EEA legal persons not subject to non-EU or non-EEA laws, and with systems and components not subject to non-EU or non-EEA laws;
- Article 4a(1)(d) to explicitly require that special categories of personal data shall only be stored, processed and handled within the EU or the EEA.

Eurosmart's comments on the Digital Omnibus on AI

Concerned text	Provision	Clause/subclause	Comments	Proposed change
Digital Omnibus Proposal for a Regulation COM(2025)836	Article 1 Amendments to Regulation (EU) 2024/1689	Article 4a - Processing of special categories of personal data for bias detection and mitigation	Eurosmart welcomes this article which will help eliminating bias in AI systems. Article 4a.1 (c) and (d) define the security measures which shall be applied for these special categories of data in that case. However, these security measures may be insufficient as they do not address the risks of these data being exported, stored or processed outside EU/EAA and thus escaping EU or Member States' control (risk of uncontrolled copying, processing for uncontrolled purpose etc.), which in turn hampers their effective security. To address this risk it shall be clarified that the entities accessing the special categories of personal data shall: • not be subject to non-EU/EEA laws be it natural or legal persons (e.g. meaning for natural persons that they shall be EU/EEA citizens); • Shall only use components (software, hardware, cloud, etc.) which are not subject to non-EU/EEA laws;	Therefore Eurosmart suggest modifying: • article 4.1(c) to include within the required measures that the special categories of personal data shall only be stored, processed and handled ○ by (1) EU/EEA natural persons and (2) EU/EEA legal persons for which it is demonstrated that they are not subject to non-EU/EEA laws; and ○ with systems and components for which it is demonstrated that they are not subject to non-EU/EEA laws; article 4.1(d) to explicitly require that the special categories of personal data shall only be stored, processed and handled within EU/EEA.

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

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 471 34 59 64 | mail Contact@eurosmart.com

EUROSMART
The Voice of the Digital Security Industry

Eurosmart's answers to Digital Omnibus public consultation

March 2026

Eurosmart, the voice of the European digital security industry, welcomes the opportunity to provide comments on the European Commission's proposal for a Digital Omnibus Regulation.

Eurosmart supports the objective of improving clarity and consistency across the EU digital regulatory framework. Ensuring legal certainty, avoiding fragmentation and facilitating practical implementation are essential for organizations operating across several Member States.

Eurosmart represents a broad membership of companies active in the European digital security sector, including providers of secure hardware, software and trusted digital solutions used across multiple industries. As providers of technologies enabling secure data processing, identity verification, authentication and cybersecurity, Eurosmart members are directly linked to the regulatory frameworks addressed in the Digital Omnibus proposal.

The digital security industry is closely involved in the implementation of several of the legislative instruments covered by this initiative, including data protection, data governance and cybersecurity frameworks. Ensuring legal clarity, regulatory coherence and practical implementation across these instruments is therefore of particular importance for our industry.

In this context, Eurosmart provides comments on several elements of the proposal, in particular on legal definitions, the processing and protection of personal data, compliance obligations under the GDPR, cybersecurity incident reporting and the interaction between different EU digital regulatory frameworks.

I. Legal clarity and definitions

Definition of "residual" personal data

Recital 33 states that special categories of personal data may residually exist in training, testing or validation datasets or may be retained in an AI system or model.

Eurosmart considers that a legal definition of the term "residual" is necessary in order to ensure legal clarity and consistent interpretation of the provision.

Definition of "residually retained data"

Article 88c refers to "residually retained data". Eurosmart considers that a definition of this term should be provided in order to ensure legal certainty and consistent interpretation of the provision.

2. Processing and protection of personal data

Processing of pseudonymized data

Eurosmart welcomes the amendment to Article 4(1) of the General Data Protection Regulation, which will help alleviate constraints for data controllers that store or process pseudonymized data.

Eurosmart also supports the introduction of Article 41a but considers that **further clarification is necessary.**

- First, the benefits of Article 41a may only apply in certain use cases or contexts. Eurosmart therefore **recommends clarifying this limitation** in Article 41a(1).
- Secondly, Article 41a(2) should include an additional element requiring the development of **criteria or categories for contexts or use cases to assess the risk of re-identification in relation to typical recipients of data**.
- Finally, Article 41a(3), as currently formulated, does not provide sufficient legal certainty. Eurosmart recommends establishing that **where entities comply with the implementing act, the data should be presumed not to enable the re-identification of data subjects**.

Processing of biometric data

The proposal introduces a derogation allowing the processing of biometric data where it is necessary to confirm the identity of a data subject.

Eurosmart considers that the wording **"is necessary"** could unintentionally restrict the scope of the derogation to cases where no alternative means of confirming identity exist. In practice, alternative means of identification are almost always available, and biometric verification should remain an option rather than an obligation for data subjects.

Eurosmart therefore recommends removing the wording **"is necessary"** and replacing it with **"is carried out".**

3. Cybersecurity and incident reporting

Alignment of incident notification timelines

Eurosmart recommends aligning the timeline for incident notifications across different EU cybersecurity and digital frameworks.

Data breaches and cybersecurity incidents are often correlated and should therefore be subject to the same notification timelines. The proposal to set the notification timelines for personal data breaches under the GDPR to 96 hours creates a discrepancy between the notification timelines of GDPR (96 hours) and other EU cybersecurity frameworks, namely the NIS2 Directive, the Digital Operational Resilience Act, and the Cyber Resilience Act, which require notifications within 72 hours.

Eurosmart therefore suggests aligning these timelines by setting the notification deadline for relevant incidents to 96 hours across the different instruments. Without such alignment, the administrative burden for essential and important entities would remain unchanged.

Interaction between NIS2 and the Cyber Resilience Act

The proposed amendment regarding the interaction between incident reporting obligations under the NIS2 Directive and the Cyber Resilience Act raises several practical questions.

In particular, clarification is needed regarding:

- the criteria used to determine whether an incident notified under the Cyber Resilience Act contains relevant information under the NIS2 Directive;
- the entity responsible for determining whether such information is relevant;
- how it will be determined whether an essential or important entity uses the affected product.

Eurosmart therefore recommends clarifying these aspects and updating the provision to ensure that incident reporting obligations apply once the conditions laid down in Article 23(1) of the NIS2 Directive are established.

4. Access to data stored in terminal equipment

Article 88a(3)(d) allows access to personal data stored in terminal equipment without consent where necessary to maintain or restore the security of a controller's service.

Eurosmart considers that the scope of this provision should be clarified, including:

1. **which entities would be entitled to access such personal data;**
2. **which operations are encompassed by the notion of maintaining or restoring security;**
3. **whether large-scale collection of personal data to identify suspicious behavior could fall under this provision.**

Clarification is also necessary to ensure that this provision remains balanced with the protection of the fundamental rights of data subjects.

5. Legitimate interests in AI development

The provision allows derogations through national laws requiring consent. Eurosmart considers that this possibility could lead to fragmentation of the digital and AI market in the EU and ultimately hamper the uptake of the EU digital industry.

Eurosmart therefore recommends **removing the possibility for Member States to introduce such derogations through national law, ensuring harmonization across the Union**.

Conclusion

Eurosmart welcomes the Digital Omnibus initiative and supports efforts to improve clarity, consistency and practical implementation of the EU digital regulatory framework.

The proposed improvements provide an opportunity to clarify key definitions, ensure legal certainty and reduce unnecessary administrative burdens while maintaining appropriate safeguards.

In particular, Eurosmart emphasizes the importance of ensuring **consistency across the different EU legislative instruments addressed by the proposal**, including the General Data Protection Regulation, the Data Act and the NIS2 Directive, as well as their interaction with other relevant frameworks such as the Cyber Resilience Act and the AI Act.

Eurosmart remains committed to engage with EU institutions in order to support the development of a coherent and effective digital regulatory framework across the European Union.

Eurosmart's comments on the Digital Omnibus

Concerned text	Provision	Clause/subclause	Comments	Proposed change
Digital Omnibus Proposal for a Regulation COM(2025)837	Recital 33		"[…] Special categories of personal data may residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model […]".	Legal definition of "residual" is necessary.
Digital Omnibus Proposal for a Regulation COM(2025)837	Recital 34		Eurosmart recommends for the definition of identification to be aligned with the AI Act. Particularly considering the following recitals and Articles: 1. Recital 14 of the AI Act: biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of biometric data includes two distinct functions, namely the identification of a natural person or the verification (also called authentication) of his or her claimed identity, both of which rely on different technical processes. 2. Recital 15 of the AI Act: "The notion of 'biometric identification' referred to in this Regulation should be defined as the automated recognition of physical,	Eurosmart recommends extending the definition present in Recital 34 to the following: **'Biometric identification' means the automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database, while 'biometric verification' means the automated, one-to-one verification, including authentication, of the identity of natural persons by comparing their biometric data to previously provided biometric data with the active involvement of the data subject.** ~~The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data~~

			physiological and behavioural human features such as the face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood pressure, odour, keystrokes characteristics, for the purpose of establishing an individual's identity by comparing biometric data of that individual to stored biometric data of individuals in a reference database, irrespective of whether the individual has given its consent or not. This excludes AI systems intended to be used for biometric verification, which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises." 3. <u>Recital 17 of the AI Act:</u> The notion of 'remote biometric identification system' referred to in this Regulation should be defined functionally, as an AI system intended for the identification of natural persons without their active involvement, typically at a distance, through the comparison of a person's biometric data with the biometric data contained in a reference database, irrespectively of the particular technology, processes or types of biometric data used. Such remote biometric identification systems are typically used to perceive multiple persons or their behaviour simultaneously in order to facilitate	~~provided by the data subject, who is thereby claiming his or her identity.~~ Derogating from the prohibition to process biometric data under Article 9(1) of the Regulation should also be allowed where the verification of the claimed identity of the data subject is **carried out** for a purpose pursued by the controller, and suitable safeguards apply to enable the data subject to have sole control of the verification process. For example, where the biometric data are securely stored solely at the side of the data subject or are securely stored at the side of the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is held solely by the data subject, that processing is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the biometric data or only for a very limited time during the verification process.

			significantly the identification of natural persons without their active involvement. This excludes AI systems intended to be used for biometric verification, which includes authentication, the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises. That exclusion is justified by the fact that such systems are likely to have a minor impact on fundamental rights of natural persons compared to the remote biometric identification systems which may be used for the processing of the biometric data of a large number of persons without their active involvement. In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems concerned by providing for minor delays. 'Real-time' systems involve the use of 'live' or 'near-live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data has already been captured and the comparison and identification occur only after a significant	

			delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned." 4. Article 3 of the AI Act provides clear definitions of 'biometric identification' (Article 3(35)) and 'biometric verification' (Article 3(36)), which should be reflected in the GDPR.	
Digital Omnibus Proposal for a Regulation COM(2025)837	Article 1 Amendments to Regulation (EU) 2023/2854 (Data Act)	Article 31(1b)	"1b. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1). Where the provider of data processing service is a small and medium-sized enterprise or a small mid-cap, the obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), if the provision of such services is based on a contract concluded before or on 12 September 2025. Where the provider of a data processing service is a small and medium-sized enterprise or a small mid-cap, the provider shall not be required to renegotiate or amend a contract for the provision of a data processing service other than those referred to in Article 30(1) before its expiry 1 if	To avoid any misinterpretation, Eurosmart believes it would be appropriate to delete the phrase "other than those referred to in Article 30(1)" from Article 31(1b). Such a clarification would help ensure legal certainty while preserving the intended balance of the Data Act.

			that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.';" As currently drafted, the provision allows providers of data processing services to include proportionate early termination penalties in fixed-term contracts but specifies "other than those referred to in Article 30(1)". This reference could create ambiguity and could potentially be interpreted as preventing such penalties for certain cloud services.	
Digital Omnibus Proposal for a Regulation COM(2025)837	Article 3 Amendments to Regulation (EU) 2016/679 (GDPR)	Article 4.1 Article 41a	Eurosmart welcomes the amendment to Article 4.1 which will help alleviating the constraints for data controllers that store or process data which are pseudonymized.	In that regard, Eurosmart also supports the newly introduced Article 41a. However, Eurosmart believes that this Article may not be sufficient to alleviate the burden while providing a clear legal framework for entities storing or processing data which are pseudonymized. • First, the benefits of Article 41a are likely to be valid for only some use cases or in some contexts. This should be considered in Article 41a.1 alongside the types of entities ("[…] certain entities"), and above all in Article 41a.2. Eurosmart therefore suggests:

				○ Appending at the end of Article 41a.1 “[…] for some use cases or in some contexts.” ○ adding in Article 41a.2 the following bullet : (3) develop criteria and or categories for contexts or use cases to assess the risk of re-identification in relation to typical recipients of data. • Secondly, Article 41a.3, as currently written, is not sufficient to provide legal certainty when complying with the content of the implementing act, which is paramount, as compliance with the implementing act “[…] may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects”. In its current formulation, this approach may limit the intended objective of reducing the burden for entities. To provide the necessary legal certainty, it would be important to establish that where an entity complies with the content of the implementing act, the data should be presumed not to enable the reidentification of data subjects. Therefore, this provision should be rewritten as follows: “Where the implementation of the means and criteria outlined in an implementing act

				are applied, it is presumed that data cannot lead to reidentification of the data subjects."
Digital Omnibus Proposal for a Regulation COM(2025)837	Article 3 Amendments to Regulation (EU) 2016/679 (GDPR)	Article 9	Commission Proposal states the following: "Article 9 [of the GDPR] is amended as follows: l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.'" Justification for the proposed amendment by Eurosmart: While the processing of biometric data for the purpose of confirming the identity of a data subject or for the purpose of identification of a data subject provides the utmost level of security – in particular in critical industries such as aviation – less secure alternative means of confirmation are always made available to data subjects. Priority should indeed be given to data subjects' right to consent to their biometric data being processed or not. As currently formulated in the Commission's proposal, the term 'necessary' may induce confusion by unintendedly restricting the scope of the derogation to cases where no alternative means of confirming the identity of the data subject exist, which, in practice, is never the case. The processing of biometric data should remain an option, not an obligation for data subjects; hence why Eurosmart proposes to remove "is necessary" from the draft article.	Eurosmart suggests the following amendment: (l) processing of biometric data is **carried out** for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject

Digital Omnibus Proposal for a Regulation COM(2025)837	Article 3 Amendments to Regulation (EU) 2016/679 (GDPR)	Article 33.1	Data breaches and incidents on network and information security are usually correlated. Therefore, to effectively reduce burden for Essential and Important Entities (established under NIS2), Eurosmart strongly suggests aligning NIS2 with the GDPR regarding the timeline for incident notification and personal data breach. If both timelines are not aligned, the burden will likely remain unchanged for Essential and Important Entities, as the timeline of 72 hours for notification – imposed by NIS2 – will still remain applicable. More precisely, the timeline for Essential and Important Entities to submit an incident notification in case of incident that has a significant impact on the provision of their services (Article 23.4(b)) should be changed to 96 hours (the current provision requires 72 hours). Likewise, for DORA (Regulation 2022/2554), the timeline for the submission of the interim report in case of major ICT-related incidents should be set to 96 hours (Article 5.1(b) of Commission Delegated Regulation (EU) 2025/301). Additionally, the same alignment should be considered for the CRA (Regulation 2024/2847) in Article 14.2(b) and Article 14.4(b).	The other acts providing for mandatory notification of cybersecurity events should be aligned with the new timeline for notification of data breaches. In particular: • Article 23.4(b) of NIS2 should be updated to set the timeline to 96 hours as for the GDPR. • Article 5.1(b) of Commission Delegated Regulation (EU) 2025/301 of DORA should be updated to set the timeline to 96 hours as for the GDPR Additionally, the same alignment should be considered for the CRA (Regulation 2024/2847) in Article 14.2(b) and Article 14.4(b).

Digital Omnibus Proposal for a Regulation COM(2025)837	Article 3 Amendments to Regulation (EU) 2016/679 (GDPR)	Article 33.1	Eurosmart welcomes this amendment which will alleviate the burden for data processors and supervisory authorities as notification to supervisory authorities would only be required in case of "[…] personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons.". This will decrease the amount of notifications sent to the supervisory authorities, which in turn will help them to focus only on "personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons."	Eurosmart supports this amendment.
Digital Omnibus Proposal for a Regulation COM(2025)837	Article 3 Amendments to Regulation (EU) 2016/679 (GDPR)	Article 35.4; 35.5;35.6	Eurosmart welcomes these provisions which will ensure harmonization at EU level regarding cases in which DPIA is required and in cases where it is not required. These will streamline conformity activities for data controllers, especially those operating across several Member States, and bring better clarity to data subjects.	Eurosmart supports these amendments.
Digital Omnibus Proposal for a Regulation COM(2025)837	Article 3 Amendments to Regulation (EU) 2016/679 (GDPR)	Article 41a	Eurosmart suggests that this Article goes a step further and requires the board to prepare and transmit to the Commission the items described in point 2, i.e.: (a) assessment of the state of the art of available techniques; (b) criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.	Recommendation to further clarify.

Digital Omnibus Proposal for a Regulation COM(2025)837	Article 3 Amendments to Regulation (EU) 2016/679 (GDPR)	Article 88a.3(d)	This Article reads the following: "(3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following: d) maintaining or restoring the security of a controller's service requested by the data subject or the terminal equipment used for the provision of such service." This provision seems to be broad and could be used a wildcard by any data controller or entity to access personal data stored in the user's terminal equipment without its consent. As such the following aspects should be better clarified: • Who would be entitled to access such personal data? • What kind of operations are encompassed by "maintaining or restoring the security of a controller's service requested by the data subject or the terminal equipment used for the provision of such service"? • Would a massive collection of personal data on mobile phones within a Member State regarding users' online behavior or usages to identify suspicious patterns (e.g. hackers) fall	Better clarify the meaning and scope of "maintaining or restoring the security of a controller's service requested by the data subject or the terminal equipment used for the provision of such service".

			under this provision of personal data collection without user consent? • Can this right be balanced by the protection of fundamental rights of data subject?	
Digital Omnibus Proposal for a Regulation COM(2025)837	Article 3 Amendments to Regulation (EU) 2016/679 (GDPR)	Article 88c First paragraph	The text reads the following: "[…] except where other Union or national laws explicitly require consent, […]" The possibility to derogate to that provision (no consent in case of legitimate interest of data controller) through national laws would lead to the fragmentation of the digital and AI market in EU. Actors based in Member States requiring consent would be disfavoured compared to the others for which the general rule would apply. As such it would be detrimental to the uptake of the AI sector in the EU, thus the development of EU actors in that sector, and ultimately to the EU autonomy and wealth. In addition, more globally this fragmentation could also impede research activities. Therefore, Eurosmart strongly suggests removing the possibility to require consent through national law. Ensuring harmonization across the EU should be done only through Union laws.	Eurosmart recommends changing the text as follows: "[…] except where other Union ~~or national~~ laws explicitly require consent, […]".

Digital Omnibus Proposal for a Regulation COM(2025)837	Article 3 Amendments to Regulation (EU) 2016/679 (GDPR)	Article 88c Second paragraph	"[…] to protect against non-disclosure of residually retained data in the AI system or AI model […]" A definition of "residually retained data" should be provided.	A definition of "residually retained data" should be provided.
Digital Omnibus Proposal for a Regulation COM(2025)837	Article 6 Amendments to Directive (EU) 2022/2555 (NIS2)	Article 23.12	This amendment clarity could be improved as it raises several questions: • On which ground and criteria will it be determined that a notification of severe incident in a product with digital elements under the CRA contains "relevant information" under Article 23 of NIS2? • Which entity will be in charge of determining whether a notification of a severe incident in a product with digital elements under the CRA contains a "relevant information" under Article 23 of NIS2? • In order to make that decision, it is necessary to know that an Essential or Important Entity uses the products with digital elements for which a severe incident under the CRA was notified. However, this information may not be known by the manufacturer or the Essential or Important Entities. How will this information be obtained? Additionally, Article 30.1 of NIS2 reads the following "In the case of a cross-border or cross-	Eurosmart recommends to: 1. Clarify the open questions. 2. Update 23.12 as follows: "When a manufacturer notifies a severe incident pursuant to Article 14(3) of Regulation (EU) 2024/2847 and the incident reporting under that Article contains relevant information as required under paragraph 4 of this Article, the reporting of the manufacturer under Article 14(3) of Regulation (EU) 2024/2847 shall constitute reporting of information under paragraph 4 of this Article once the conditions laid down in Article 23.1 [of NIS2] for their collection and use are established."

			sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.”. Therefore, notification of severe incident in a product with digital elements under the CRA shall only be collected and used as “relevant information” when it is established first that (1) a significant incident impacts an Essential or Important Entities and (2) that it is cross border or cross sectorial. Still, the amendment does not indicate these prerequisites, which should be clarified in the amendment.	

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

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 471 34 59 64 | mail Contact@eurosmart.com